

VISIT...

LANZAROTE  
*Caliente*.COM

# The Handbook of Information Security for Advanced Neuroprosthetics

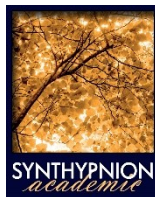


Matthew E. Gladden

# The Handbook of Information Security for Advanced Neuroprosthetics

Matthew E. Gladden

a volume in the series on  
**Posthuman Technologies and  
Organizational Management**



The Handbook of Information Security for Advanced Neuroprosthetics  
Copyright © 2015 Matthew E. Gladden

Volume 1 in the Series on Posthuman Technologies and Organizational  
Management

Published in the United States of America  
by Synthypnion Academic in association with West Pole & Larkspur,  
imprints of Synthypnion Press, LLC

All rights reserved. No part of this publication may be reproduced, stored in  
a retrieval system, or transmitted in any form or any means, electronic, me-  
chanical, photocopying, recording, or otherwise, without the prior permis-  
sion of the publisher, apart from those fair-use purposes permitted by law.

Synthypnion Press, LLC  
Indianapolis, IN 46227  
<http://www.synthypnionpress.com>



ISBN 978-0-692-50161-0

10 9 8 7 6 5 4 3 2

August 2015

*To all those who make use of these technologies,  
whether out of necessity or by choice –  
that such tools might be sources of health,  
freedom, and full human development.*

## Brief Table of Contents

|                                                                                                        |            |
|--------------------------------------------------------------------------------------------------------|------------|
| <b>Acknowledgements .....</b>                                                                          | <b>10</b>  |
| <b>Part I: Background and Foundations .....</b>                                                        | <b>13</b>  |
| The Purpose and Organization of This Text .....                                                        | 15         |
| Chapter 1: An Introduction to Advanced Neuroprosthetics.....                                           | 19         |
| Chapter 2: An Introduction to Information Security in the Context<br>of Advanced Neuroprosthetics..... | 39         |
| Chapter 3: Critical Challenges in Information Security for<br>Advanced Neuroprosthetics .....          | 59         |
| <b>Part II: Developing New Conceptual Frameworks.....</b>                                              | <b>105</b> |
| Chapter 4: An Information Security Device Ontology for<br>Advanced Neuroprosthetics .....              | 107        |
| Chapter 5: A Two-dimensional Framework of Cognitive Security<br>for Advanced Neuroprosthetics .....    | 129        |
| <b>Part III: Security Practices and Mechanisms for Advanced<br/>Neuroprosthetics .....</b>             | <b>169</b> |
| Chapter 6: Responsibility for Security Planning and<br>Implementation .....                            | 171        |
| Chapter 7: Management Controls for Advanced Neuroprosthetics .....                                     | 205        |
| Chapter 8: Operational Controls for Advanced Neuroprosthetics .....                                    | 223        |
| Chapter 9: Technical Controls for Advanced Neuroprosthetics.....                                       | 267        |
| <b>Part IV: Appendix .....</b>                                                                         | <b>305</b> |
| Biocybernetic Classification of Advanced Neuroprosthetic Devices ....                                  | 306        |
| <b>Bibliography .....</b>                                                                              | <b>326</b> |
| <b>Index .....</b>                                                                                     | <b>349</b> |



# Detailed Table of Contents

**Acknowledgements .....10**

**Part I: Background and Foundations ..... 13**

    The Purpose and Organization of This Text ..... 15

    Chapter 1: An Introduction to Advanced Neuroprosthetics..... 19

        Overview of current neuroprosthetic devices ..... 19

*Neuroprosthetic devices categorized by function* ..... 22

*Neuroprosthetic devices categorized by purpose: therapy vs. enhancement* ..... 28

*Neuroprosthetic devices categorized by physical location: implant vs. prosthesis* ..... 28

*Neuroprosthetic devices categorized by agency: active vs. passive* ..... 30

*Implantable computers vs. neuroprosthetic devices*..... 32

        Expected developments in neuroprosthetics: toward posthuman enhancement ..... 32

*Early adopters of neuroprosthetic devices for posthuman enhancement* ..... 34

*Neuroprosthetic devices categorized by cybernetic characteristics: reality, virtuality, xenosomatics, and hive minds* ..... 34

*The meaning of “advanced” neuroprosthetics*..... 36

    Chapter 2: An Introduction to Information Security in the Context of Advanced Neuroprosthetics..... 39

        Institutional processes and personal practices..... 39

        The CIA Triad ..... 39

        Security controls..... 40

*An example of administrative, logical, and physical controls*..... 41

*Overlap of different kinds of security controls*..... 43

        Authentication and authorization ..... 44

        Vulnerabilities, threats, and risks ..... 45

*Classifying vulnerabilities, threat sources, and threats* ..... 48

    Chapter 3: Critical Challenges in Information Security for Advanced Neuroprosthetics ..... 59

|                                                                                                                                  |     |
|----------------------------------------------------------------------------------------------------------------------------------|-----|
| Information security considerations unique to advanced neuroprosthetics.....                                                     | 59  |
| <i>Device user vs. device host</i> .....                                                                                         | 59  |
| <i>Critical, noncritical, or no health impacts for a device's host and user</i> .....                                            | 62  |
| <i>Lack of direct physical access to implanted systems</i> .....                                                                 | 64  |
| <i>100% availability required</i> .....                                                                                          | 65  |
| <i>The need for rigorous security vs. the need for instant emergency access</i> .....                                            | 69  |
| <i>Securing a neuroprosthetic device vs. securing a neurocybernetic device-host system</i> .....                                 | 80  |
| <i>The weakest link – now at the heart of an information system</i> .....                                                        | 81  |
| <i>New kinds of information systems to be protected – or used in executing attacks</i> .....                                     | 83  |
| <i>New possibilities for biometrics</i> .....                                                                                    | 84  |
| <i>Nontraditional computing platforms: from biomolecular computing and neural networks to nanorobotic swarms</i> .....           | 92  |
| <i>Technology generating posthuman societies and posthuman concerns</i> .....                                                    | 94  |
| <i>Human autonomy, authenticity, and consciousness: risk management and the possibility of ultimate loss</i> .....               | 96  |
| <i>A growing nexus of information security, medicine, biomedical engineering, neuroscience, and cybernetics</i> .....            | 100 |
| The need for new conceptual frameworks: ontologies, typologies, and protocols for information security for neuroprosthetics..... | 102 |

## **Part II: Developing New Conceptual Frameworks..... 105**

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| Chapter 4: An Information Security Device Ontology for Advanced Neuroprosthetics ..... | 107 |
| Introduction to the ontology .....                                                     | 107 |
| First area: context and relations .....                                                | 109 |
| <i>Human agents</i> .....                                                              | 109 |
| <i>Factors impacting availability</i> .....                                            | 111 |
| <i>Physiological context</i> .....                                                     | 112 |
| Second area: physical components.....                                                  | 113 |
| <i>Device morphology</i> .....                                                         | 113 |
| <i>Input mechanisms: physical receivers of matter, energy, and information</i> .....   | 114 |
| <i>Output mechanisms: physical emitters of matter, energy, and information</i> .....   | 115 |
| <i>Computational substrate</i> .....                                                   | 116 |
| Third area: processes.....                                                             | 117 |
| <i>Computational processes and computer control</i> .....                              | 117 |
| <i>Input modalities and signals interpretable by the device</i> .....                  | 119 |



|                                                                                                               |            |
|---------------------------------------------------------------------------------------------------------------|------------|
| <i>Output modalities and signals expressible by the device .....</i>                                          | <i>121</i> |
| Fourth area: data, information, and knowledge received, generated,<br>stored, and transmitted .....           | 123        |
| <i>Data regarding the device's status and diagnostics .....</i>                                               | <i>123</i> |
| <i>Environmental data .....</i>                                                                               | <i>123</i> |
| <i>Data regarding the host's physical status and biological processes.....</i>                                | <i>124</i> |
| <i>Data regarding the host's cognitive activity and patterns .....</i>                                        | <i>124</i> |
| <i>Procedural knowledge.....</i>                                                                              | <i>125</i> |
| <i>Declarative knowledge.....</i>                                                                             | <i>125</i> |
| Toward developing a comprehensive information security framework .....                                        | 126        |
| <b>Chapter 5: A Two-dimensional Framework of Cognitional Security<br/>for Advanced Neuroprosthetics .....</b> | <b>129</b> |
| Developing a two-dimensional cognitional security framework.....                                              | 129        |
| Defining security goals for the entire device-host system: nine essential<br>attributes.....                  | 129        |
| <i>Confidentiality .....</i>                                                                                  | <i>130</i> |
| <i>Integrity.....</i>                                                                                         | <i>132</i> |
| <i>Availability .....</i>                                                                                     | <i>133</i> |
| <i>Possession .....</i>                                                                                       | <i>134</i> |
| <i>Authenticity .....</i>                                                                                     | <i>135</i> |
| <i>Utility .....</i>                                                                                          | <i>136</i> |
| <i>Distinguishability .....</i>                                                                               | <i>138</i> |
| <i>Rejectability.....</i>                                                                                     | <i>139</i> |
| <i>Autonomy.....</i>                                                                                          | <i>139</i> |
| Prioritizing the information security goals.....                                                              | 142        |
| Understanding the security goals at three levels .....                                                        | 145        |
| <i>Functional vs. information security impacts .....</i>                                                      | <i>147</i> |
| <i>Impacts on a host vs. impacts on a user.....</i>                                                           | <i>147</i> |
| <i>The human host as sapient metavolitional agent.....</i>                                                    | <i>147</i> |
| <i>The host as embodied embedded organism.....</i>                                                            | <i>155</i> |
| <i>The host as social and economic actor.....</i>                                                             | <i>159</i> |
| Conclusion .....                                                                                              | 168        |

## **Part III: Security Practices and Mechanisms for Advanced Neuroprosthetics..... 169**

|                                                                                     |            |
|-------------------------------------------------------------------------------------|------------|
| <b>Chapter 6: Responsibility for Security Planning and<br/>Implementation .....</b> | <b>171</b> |
| Overview of security activities .....                                               | 171        |
| <i>Initiation phase.....</i>                                                        | <i>172</i> |
| <i>Development and acquisition phase.....</i>                                       | <i>173</i> |

|                                                                                                |            |
|------------------------------------------------------------------------------------------------|------------|
| <i>Implementation phase</i> .....                                                              | 176        |
| <i>Operations and maintenance phase</i> .....                                                  | 178        |
| <i>Disposal phase</i> .....                                                                    | 180        |
| Roles and responsibilities for information security .....                                      | 181        |
| <i>Individuals and organizations participating in an advanced neuroprosthetic system</i> ..... | 181        |
| <i>Typical formalization of roles and responsibilities in an institutional setting</i> .....   | 191        |
| <i>Potential specialized roles for future neuroprosthetic systems</i> .....                    | 198        |
| <i>Multiple roles for a single individual?</i> .....                                           | 202        |
| <i>Roles and responsibilities for nonhuman agents?</i> .....                                   | 202        |
| Conclusion .....                                                                               | 203        |
| Chapter 7: Management Controls for Advanced Neuroprosthetics .....                             | 205        |
| Risk assessment .....                                                                          | 206        |
| Planning .....                                                                                 | 208        |
| System and services acquisition .....                                                          | 211        |
| Certification, accreditation, and security assessments .....                                   | 221        |
| Chapter 8: Operational Controls for Advanced Neuroprosthetics .....                            | 223        |
| Personnel security .....                                                                       | 224        |
| Physical and environmental protection .....                                                    | 227        |
| Contingency planning .....                                                                     | 234        |
| Configuration management .....                                                                 | 237        |
| Maintenance .....                                                                              | 240        |
| System and information integrity .....                                                         | 241        |
| Media protection .....                                                                         | 259        |
| Incident response .....                                                                        | 261        |
| Awareness and training .....                                                                   | 265        |
| Chapter 9: Technical Controls for Advanced Neuroprosthetics .....                              | 267        |
| Identification and authentication .....                                                        | 268        |
| Access control .....                                                                           | 273        |
| Audit and accountability .....                                                                 | 280        |
| System and communications protection .....                                                     | 282        |
| <b>Part IV: Appendix .....</b>                                                                 | <b>305</b> |
| Biocybernetic Classification of Advanced Neuroprosthetic Devices ....                          | 306        |
| Summary .....                                                                                  | 306        |
| Cybernetic implications .....                                                                  | 306        |

|                                                                  |            |
|------------------------------------------------------------------|------------|
| Importance for information security.....                         | 307        |
| Classification of neuroprosthetic devices by neural process..... | 307        |
| <i>Sensory neuroprosthetic devices</i> .....                     | 307        |
| <i>Cognitive neuroprosthetic devices</i> .....                   | 316        |
| <i>Motor neuroprosthetic devices</i> .....                       | 320        |
| <b>Bibliography .....</b>                                        | <b>326</b> |
| <b>Index .....</b>                                               | <b>349</b> |

## Acknowledgements

Throughout the process of researching and writing this book, I have benefitted from the input and support of many individuals who contributed in one way or another to the successful completion of this project. Among that group are many scholars who have shared questions, feedback, and suggestions at the conferences at which I presented material that was eventually incorporated into this text. For the insights that they have shared I would especially like to thank Bartosz Kłoda-Staniecko, Magdalena Szczepocka, Michał Kłosiński, Agata Kowalewska, Piotr Toczyski, Alan N. Shapiro, Krzysztof Maj, Katarzyna Marak, Miłosz Markocki, Jakub Krogulec, Dawid Junke, and Sven Dwulecki. I am also grateful to all the faculty, administrators, and library staff of the Institute of Computer Science of the Polish Academy of Sciences, particularly Serge Pukas and Paulina Krystosiak, who provided me with much encouragement in my research, and Robert Pająk, who offered a number of valuable insights and questions during my research for this book.

I am also grateful to the faculty and staff of Georgetown University's School of Continuing Studies, especially Edwin Schmierer and Douglas McCabe, and to the current and former faculty and staff of the University's Department of Psychology at Georgetown University, especially Brad Kelly, Aisulu Raspayeva, and James Lamiell. I would also like to thank all of the research fellows and staff with whom I worked at the Woodstock Theological Center, particularly Keelan Downton, Maria Ferrara, Kevin Flannery, Madeline Howard, Matthew Hummer, Christian Lambert, John McKelvie, Laura Michener, Marley Moynahan, Mariann Payne, Tessa Pulaski, Harry Risetto, Rita Rodriguez, Sarah Stern, Nancy Swartz, Kathryn Tucker, David Wilkins, and many others. I am especially indebted to Father John Haughey, S.J., for his stalwart encouragement and his insights relating to transhumanism and theology; to Terry Armstrong for his generous encouragement, his knowledge of artificial intelligence and organizational management, and his good example; and to Father Gap Lo Biondo, S.J., for more than the printed page can contain.

I am also thankful to friends and colleagues such as AJ Johnson and Nathan Fouts, with whom I enjoyed helpful conversations about topics of cybernetics, posthumanism, and information security whose fruits have found a home in this text. I am grateful to Tom Rijntjes for his inspiring example of ingenuity, intellectual entrepreneurship, and tireless labor. I owe a boundless debt to my parents and my brother for their unceasing encouragement and support. I am also grateful to Trigonometry Team Associates for their assistance with the formatting of this text and especially to Bogna J. Obidzińska and the editorial staff of West Pole & Larkspur and Synthypon Academic for all of their advice and support. Finally, I thank all of those whom I have forgotten to mention by name not because their contribution was so slight but because it was so great that I have come to take it (and them) for granted.

Together, all of the individuals mentioned above have made it possible for me to prepare this book; they have contributed immensely to whatever value this text might hold for those concerned about information security for advanced neuroprosthetic devices and systems. Whatever flaws, biases, and limitations the book may possess are the fault not of any of the persons mentioned above but are my responsibility alone.



## Part I

# Background and Foundations





## The Purpose and Organization of This Text

How can one provide adequate information security for a device that is integrated into the neural processes of a human mind – and perhaps more importantly, how can one provide adequate information security for that mind itself? That is the essential question that has given rise to this book, which is the first text dedicated to studying the issue comprehensively from both theoretical and practical perspectives.

The material presented in this volume is organized into three main parts plus an appendix. The first part of this book provides an introduction to key themes and questions that provide the foundation for the entire text and which will recur throughout the volume in many different contexts. In **Chapter One**, we present an introduction to neuroprosthetic devices and systems that explores both the state of the art of sensory, motor, and cognitive neuroprosthetic devices that are currently in use as well as more sophisticated kinds of neuroprosthetic technologies that are being actively pursued or are expected to be developed in the future. This overview takes us from the contemporary world of neuroprosthetic devices that have been designed primarily for purposes of therapeutic treatment of medical disorders and the restoration of natural human abilities lost due to illness or injury to an emerging future world in which neuroprosthetic devices offer the possibility of augmenting and transforming the capacities of their users in such a way that they can perhaps best be described as “transhuman” or “posthuman.” In **Chapter Two**, we present an introduction to basic principles and practices within the complex, diverse, and dynamic field of information security. Concepts such as the CIA Triad; the nature of administrative, logical, and physical security controls; the role of access controls in performing user authentication and authorization; and the differences between vulnerabilities, threats, and risks are all discussed. We also highlight the different forms that information security can take when pursued by a large organization as opposed to, say, the individual user of a consumer electronics device. In **Chapter Three**, we con-

sider unique challenges, problems, and opportunities that arise when one attempts to apply the general principles and practices of information security to the somewhat idiosyncratic domain of advanced neuroprosthetics. Issues discussed include the distinction between a device and its device-host system; the need for a device to provide free access to outside parties during medical emergencies while rigorously restricting access outside parties at other times; challenges that arise relating to implanted devices' limited power supply and processing and storage capacities, physical inaccessibility, and reliance on wireless communication; new kinds of biometrics that can be utilized by neuroprosthetic devices; complications and opportunities arising from the use of nontraditional computing structures and platforms such as biomolecular computing and nanorobotic swarms; and psychological, social, and ethical concerns that arise relating to the agency, autonomy, and personal identity of human beings possessing advanced neuroprosthetic devices. Having considered such issues, we discuss why traditional concepts of information security that are often applied to general-purpose computing and information systems are inadequate to address the realities of advanced neuroprosthetic device-host systems and why the creation of new specialized conceptual models of information security for advanced neuroprosthetics is urgently required.

The second part of the text presents two new conceptual frameworks designed to aid us in understanding the information security of advanced neuroprosthetic devices and systems and developing effective information security practices and mechanisms that are tailored to the unique needs and capacities of such systems. In **Chapter Four** we outline a device ontology for advanced neuroprosthetic devices that is designed specifically with information security in mind. The ontology allows a structured description, comparison, and analysis of neuroprosthetic devices that takes into account a device's context and relations; physical components; processes; and the kinds of data and information that are received, generated, stored, or transmitted by the device.

In **Chapter Five** we develop a two-dimensional cognitional security framework for advanced neuroprosthetic devices that takes into account not only the information security needs of a neuroprosthetic device itself but also those of the device-host system that the device creates through its integration into the neural circuitry of its human host. The framework first describes nine information security goals or attributes – namely, confidentiality, integrity, availability, possession, authenticity, utility, distinguishability, rejectability, and autonomy. This framework shares some common elements with classical

models of information security goals that were formulated for general-purpose computing and information systems, but it also proposes new elements to address the unique nature of advanced neuroprosthetic devices. The framework considers how the pursuit of these security goals for a device-host system can be advanced (or subverted) at three different levels, in which the human host of a neuroprosthetic device is considered in his or her role as: 1) a sapient metavolitional agent; 2) an embodied embedded organism; and 3) a social and economic actor.

The third part of the book discusses practical aspects of developing and implementing information system security plans for advanced neuroprosthetic devices, either within the context of a large organization or for an individual consumer who is utilizing such a device. In **Chapter Six** we describe how responsibilities for planning and implementing information security practices and mechanisms are typically allocated among individuals filling different roles. We then note the unique forms that these roles and responsibilities can take when the focus of their activities is ensuring information security for advanced neuroprosthetics. The next three chapters explore how security controls relate to advanced neuroprosthetic devices and systems by considering in detail the families of controls listed *NIST Special Publication 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations*, produced by the National Institute of Standards & Technology in 2013. We address most of the security controls noted in *NIST SP 800-53*, explaining how particular controls that were designed for use with general-purpose computing and information systems may either: 1) become *more critical* for ensuring information security when the information system to which the control is being applied is an advanced neuroprosthetic device; 2) become *less important* or potentially even irrelevant and inapplicable within the context of an advanced neuroprosthetic device; or 3) may take on *new and radically* different forms when applied to advanced neuroprosthetic devices. **Chapter Seven** focuses on management controls, **Chapter Eight** considers operational controls, and **Chapter Nine** addresses technical controls.

Finally, in the **Appendix** we present a biocybernetic model for classifying and describing advanced neuroprosthetic devices according to the neural processes in which they participate and the roles that they play in those processes – and in particular, roles involving communication and control. The classification scheme is designed to be broad enough to apply both to all kinds of neuroprosthetic devices that are currently in use as well as radically different and unconventional forms of neuroprosthetic devices that have been proposed or are expected to someday be developed.

As the first book dedicated to studying these issues comprehensively from both theoretical and practical perspectives, this volume is intended to serve

as a textbook for specialized studies in information security, cybernetics, bioethics, and biotechnology; as reference for researchers and practitioners working to ensure information security for advanced neuroprosthetics; and as a starting point for all those who are seeking to explore the subject and are in search of practical and conceptual frameworks that can guide the development of this emerging field.

## Chapter One

# An Introduction to Advanced Neuroprosthetics

### Overview of current neuroprosthetic devices

The integration of human beings with computers at both the physical and cognitive levels grows ever deeper, as new technologies are developed and the daily routines of our human existence adapt to incorporate these new means of experiencing and shaping reality. Traditionally, **human-computer interaction (HCI)** has relied on tools that are external to the human body, such as keyboards, mice, computer screens, and speakers. In recent years, however, the emergence of mobile and wearable technologies such as smartphones, smartwatches, and virtual reality headsets has created a new range of devices that are more intimately connected with the bodies of their human users. But for a growing population of persons, computerized information systems are no longer technologies that simply exist outside of – or even on the surface of – their bodies; for these persons, computing technologies have passed through the boundaries of the human body and have come to exist and to operate within their physical being. For example, an increasing number of human beings now house within their bodies implantable computers that are active and functioning continually as those persons go about their everyday activities. Such implantable computers often form key components of implantable medical devices (IMDs) such as defibrillators, pacemakers, deep brain stimulators, retinal and cochlear implants, or diagnostic devices such as body area networks (BANs) or body sensor networks (BSNs). Some of the more sophisticated forms of implantable RFID transponders also function as implantable computers.<sup>1</sup> Such implantable computers are increasingly serving as sites for the reception, generation, storage, processing, and transmission of large quantities of highly sensitive information<sup>2</sup> regarding almost every aspect of the lives of their human hosts, including their

---

<sup>1</sup> See Gasson et al., “Human ITC Implants: From Invasive to Pervasive” (2012), and Gasson, “Human ICT Implants: From Restorative Applications to Human Enhancement” (2008).

<sup>2</sup> See Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the

hosts' everyday interactions with the environment (including interactions with other human beings), their internal biological processes, and even their cognitive activity.

One kind of computer that becomes linked with a particular human being's organism in an especially powerful and intimate way is a **neuroprosthetic device** that is integrated directly into the body's neural circuitry.<sup>3</sup> A neuroprosthetic device may either be physically inserted into the brain, as in the case of many kinds of brain implants already in use, or it could potentially surround the brain, as in the case of a full cyborg body of the sort envisioned by some researchers and futurologists.<sup>4</sup> Neuroprosthetic devices increasingly operate in rich and complex biocybernetic and neurocybernetic control loops with the body and mind of their human host, allowing the host's cognitive activity to be detected, analyzed, and interpreted for use in exercising real-time control over computers or robotic devices.<sup>5</sup>

The terminology used to describe such devices is still quite fluid and not always precise, evolving rapidly alongside the underlying technologies. Lebedev notes that while particular terms may be more appropriate in specific circumstances, neuroprosthetic devices and systems are often described interchangeably as "brain-machine interfaces" (or BMIs), "neural prostheses, brain-computer interfaces (BCIs), neural interfaces, mind-machine interfaces and brain implants."<sup>6</sup> The design and use of such devices can be understood as a subfield of operative neuromodulation, which involves "altering electri-

---

Use of Human ICT Implants" (2012); Li et al., "Advances and Challenges in Body Area Network" (2011); and Rotter & Gasson, "Implantable Medical Devices: Privacy and Security Concerns" (2012).

<sup>3</sup> For a discussion of circuit models as they apply to neural information processing, see Ma et al., "Circuit Models for Neural Information Processing" (2005). For the challenges involved with designing electrodes and other implantable electronic devices or structures that can create a sustainable interface with individual neurons, see Passeraub & Thakor, "Interfacing Neural Tissue with Microsystems" (2005). For a discussion of different technologies that are used to interface electronic systems with peripheral nerves (e.g., cuff, hook, or helix electrodes) or cortical neurons (e.g., needle arrays), see Koch, "Neural Prostheses and Biomedical Microsystems in Neurological Rehabilitation" (2007). Emerging technologies such as optogenetics used to modulate neuronal firing may make it possible to solve (or avoid) some problems relating to biocompatibility and the degradation of tissues and electrodes experienced with conventional implanted electrode systems; see Humphreys et al., "Long Term Modulation and Control of Neuronal Firing in Excitable Tissue Using Optogenetics" (2011).

<sup>4</sup> See Lebedev, "Brain-Machine Interfaces: An Overview" (2014), p. 99.

<sup>5</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); Park et al., "The Future of Neural Interface Technology" (2009).

<sup>6</sup> See Lebedev, "Brain-Machine Interfaces: An Overview" (2014), p. 99.

cally or chemically the signal transmission in the nervous system by implanted devices in order to excite, inhibit or tune the activities of neurons or neural networks” – something that is done typically (at least, at present) to produce therapeutic effects.<sup>7</sup> Drawing on definitions offered by Lebedev<sup>8</sup> and others, for the purposes of this text we can define a neuroprosthetic device as **a technological device that is integrated into the neural circuitry of a human being**. Such a definition is intentionally broad and simple; at the same time, it is specific enough to exclude some kinds of devices that might be considered “neuroprosthetic devices by” other authors writing in different contexts. We can note some key implications of our definition as it will be employed in this text:

- As defined above, a neuroprosthetic device does not need to be physically implanted within the body of a human host; in principle, it could function outside of its host’s body (e.g., as a wearable device).
- The neuroprosthetic device must, however, be “integrated into” the neural circuitry of its human host. This requirement for integration entails a relatively rich and stable systematic connection between the device and some neurons within the host’s body. An fMRI machine, for example, would thus typically not qualify as a “neuroprosthetic device,” because despite the large amount of information that it generates regarding the neural activity of its host – and the effect of its magnetic field on the brain – it is not “integrated into” the host’s neural circuitry.
- In order for a neuroprosthetic device to be integrated into the neural circuitry of its human host, it is not sufficient for the device to physically adjoin particular neurons or even to be completely surrounded by the host’s neurons; rather there must be some functional interaction between the device and neurons in the host’s body. Such interaction does not need to be bidirectional: an artificial retina, for example, might generate and transmit an electrochemical stimulus that affects adjacent neurons while not being able to register or receive any stimulus from those neurons in return.
- A neuroprosthetic device does not need to be connected to neurons in its host’s *brain*. While some existing kinds of neuroprosthetic devices indeed possess a physical interface with interneurons found in the gray matter of the human brain, a neuroprosthetic device might instead be connected to sensory or motor neurons located in limbs, sensory organs, or other parts of the body.

---

<sup>7</sup> See Sakas et al., “An Introduction to Neural Networks Surgery...” (2007).

<sup>8</sup> See Lebedev, “Brain-Machine Interfaces: An Overview” (2014).



- A neuroprosthetic device does not need to be electronic in nature. Ongoing developments in fields such as genetic engineering, synthetic biology, bionanotechnology, and biomolecular computing are opening the door to the creation of neuroprosthetic devices that are partially or wholly composed of biological material (perhaps based on the DNA of the device's host) or other components.<sup>9</sup> It must, however, be a "device" that has been developed through the use of some specific technology; in the absence of specific augmentations or modifications, a limb or organ that has simply been transplanted from another human being into its new human host would generally not qualify as a neuroprosthetic device.

## Neuroprosthetic devices categorized by function

Existing kinds of neuroprosthetic devices have been categorized in different ways.<sup>10</sup> For example, a neuroprosthetic device can be classified based on the nature of its interface with the brain's neural circuitry as either **sensory**, **motor**, **bidirectional sensorimotor**, or **cognitive**.<sup>11</sup> We can consider each of these types of devices in turn.

### SENSORY NEUROPROSTHETICS

A sensory neuroprosthetic device is a neuroprosthetic device whose function is to present sense data to the mind of the device's human host,<sup>12</sup> which

---

<sup>9</sup> For a hybrid biological-electronic interface device (or "cultured probe") that includes a network of cultured neurons on a planar substrate, see Rutten et al., "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe" (2007). As Rutten et al. note, such a cultured neural network would not only serve as a link between the interface's electronic components and natural neurons within the host's body but could potentially carry out its own specialized information-processing functions. Hybrid biological-electronic interface devices are also discussed by Stieglitz in "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems" (2007).

<sup>10</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>11</sup> See Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>12</sup> See Lebedev, "Brain-Machine Interfaces: An Overview" (2014), and Troyk & Cogan, "Sensory Neural Prostheses" (2005).

we can refer to as the device's "hostmind."<sup>13</sup> Typical kinds of sensory neuroprosthetics that are already in use include cochlear implants, auditory brainstem implants,<sup>14</sup> and artificial retinas.<sup>15</sup>

Sensory neuroprosthetics may participate in different stages of the hostmind's process of acquiring and perceiving sensory information. Some sensory neuroprosthetics perform, participate in, or support the acquisition of raw sense data from distal stimuli. For example, an artificial retina that registers the arrival of photons from the external environment and then electrically stimulates the host's natural biological retinal ganglion cells is filling such a role.

Other sensory neuroprosthetics may perform the function of transmitting, translating, or transducing electrochemical signals bearing sensory information that are already present within the hostmind's body. For example, if the retina of a human subject is still intact but part of the attached optic nerve has been damaged, a sensory neuroprosthetic could replace a portion of the optic nerve in performing the task of carrying signals from the retina to the brain. Alternatively, a sensory neuroprosthetic could be used to translate sense data from one sensory modality to another:<sup>16</sup> for example, auditory sense data received by hair cells in the inner ear or by a cochlear implant could be translated by the neuroprosthetic device into signals that are supplied to the optic nerve, thereby causing the incoming sounds not to be "heard" by the hostmind through the sensory modality of hearing but instead to be "seen" through the sensory modality of vision – with the sounds perhaps appearing as patterns of light within a small portion of the hostmind's field of vision, thereby creating a form of visual augmented reality.

Yet other kinds of sensory neuroprosthetics might directly stimulate portions of the brain to create a particular sensory experience. For example, in the case of a human being whose optic nerve is destroyed or absent, a neuroprosthetic implant that is interconnected with neurons of a host's lateral geniculate nucleus or visual cortex could – by directly stimulating those areas – potentially cause the hostmind to experience visual phenomena that were not caused by any stimuli or signals present in the retina or optic nerve and which

---

<sup>13</sup> In this text we will often refer to the mind of a neuroprosthetic device's human host as the device's "hostmind" in order to indicate that we are describing the host's cognitive activity primarily from the perspective of his or her subjective sapient awareness and conscious experience rather than at the cellular or molecular level of biochemical processes occurring within the brain.

<sup>14</sup> See Cervera-Paz et al., "Auditory Brainstem Implants: Past, Present and Future Prospects" (2007).

<sup>15</sup> See Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012).

<sup>16</sup> This possibility was foreseen by cyberneticists as early as the 1940s. See Wiener, *Cybernetics* (1961), loc. 2784ff, and Lebedev, "Brain-Machine Interfaces: An Overview" (2014), p. 106.

may not correspond to any distal stimuli existing in the external environment.<sup>17</sup> Data transmitted wirelessly to such an implant from an external computer could allow the hostmind to experience either sense data corresponding to the “real” environment existing outside the host’s body or corresponding to some entirely “virtual” environment whose characteristics are created and maintained by software within the computer.

In all of these cases, the common trait is the fact that sensory neuroprosthetic devices are helping to present sense data to the mind of the devices’ human host.

### **MOTOR NEUROPROSTHETICS**

Motor neuroprosthetics, conversely, are devices that convey motor instructions – typically either from their human host’s brain or from the device’s own computer that is acting as a surrogate for the host’s brain – to some organ, device, or system within or outside of the host’s body for physical actuation.<sup>18</sup> Devices of this sort are already being used to fill a wide range of roles in treating diverse medical conditions and providing therapeutic benefits to many people around the world. For example, motor neuroprosthetics are capable of detecting and interpreting their user’s thoughts in order to allow the user to steer a wheelchair or guide a cursor around a computer screen.<sup>19</sup> They can provide life-altering benefits as the only means of communication with the outside world for locked-in patients who are completely paralyzed yet fully conscious, including those suffering from ALS, stroke, or traumatic brain injury.<sup>20</sup> They are also used to control internal bodily actions – for example, to restore bladder function after spinal cord injury, eliminate the need for an external ventilator in severely paralyzed individuals, or stimulate nerves that coordinate breathing and swallowing reflexes in order treat sleep apnea or facilitate swallowing after a stroke.<sup>21</sup> Motor neuroprosthetics

---

<sup>17</sup> For the possibility of visual cortical implants, see Thanos et al., “Implantable Visual Prostheses” (2007).

<sup>18</sup> See Lebedev, “Brain-Machine Interfaces: An Overview” (2014), and Patil & Turner, “The Development of Brain-Machine Interface Neuroprosthetic Devices” (2008).

<sup>19</sup> See Edlinger et al., “Brain Computer Interface” (2011); Lebedev, “Brain-Machine Interfaces: An Overview” (2014); Merkel et al., “Central Neural Prostheses” (2007); and Widge et al., “Direct Neural Control of Anatomically Correct Robotic Hands” (2010).

<sup>20</sup> See Donchin & Arbel, “P300 Based Brain Computer Interfaces: A Progress Report” (2009).

<sup>21</sup> See Taylor, “Functional Electrical Stimulation and Rehabilitation Applications of BCIs” (2008).

can also potentially be used to predict<sup>22</sup> or stop<sup>23</sup> epileptic seizures. They can be used for functional electrical stimulation (FES) to restore muscle functionality to individuals suffering from paralysis<sup>24</sup> (either as a permanent assistive technology or temporary rehabilitative tool<sup>25</sup>), to treat central hypoventilation syndrome,<sup>26</sup> and for neurally augmented sexual function (NASF) to restore or improve sexual function in both male and female subjects.<sup>27</sup> Meanwhile, the use of BCI devices for vagus nerve stimulation (VNS) has been explored or considered to treat conditions such as Alzheimer's disease, anxiety disorders, bulimia, addictions, and narcolepsy.<sup>28</sup> Nontherapeutic applications of motor brain-computer interface (BCI) technologies have included, for example, the use of an EEG-based BCI to allow its human operator to drive a car in a 3D virtual reality environment.<sup>29</sup>

Some motor neuroprosthetics are implanted in or interface with neurons in their host's brain, detecting neuronal activity that relates to a conscious volition or unconscious motor instruction and translating that activity into an output stimulus or signal produced by the device that activates or informs the functioning of transmission mechanisms that carry instructions to the motor plants or actuators that ultimately manifest the motor action. Other motor neuroprosthetics directly perform the work of transmitting such instruction-bearing stimuli to a motor plant or actuator (in the human organism, typically via a neuroeffector junction); still others receive and interpret such instructions and then execute the intended action through control of a motor plant, motor organ, or actuator. Technologies that can be used to detect intent manifested within a human include electroencephalography (EEG), electrocorticography (ECoG), recordings of local field potentials (LFPs), and recordings of single-neuron action potentials,<sup>30</sup> as well as functional near infrared spectroscopy (fNIR).<sup>31</sup> Each technology has its unique

---

<sup>22</sup> For the use of EEG-based systems for this purpose, see Drongelen et al., "Seizure Prediction in Epilepsy" (2005).

<sup>23</sup> See Fountas & Smith, "A Novel Closed-Loop Stimulation System in the Control of Focal, Medically Refractory Epilepsy" (2007).

<sup>24</sup> See Durand et al., "Electrical Stimulation of the Neuromuscular System" (2005), and Moxon, "Neurorobotics" (2005).

<sup>25</sup> See Masani & Popovic, "Functional Electrical Stimulation in Rehabilitation and Neurorehabilitation" (2011).

<sup>26</sup> See Taira & Hori, "Diaphragm Pacing with a Spinal Cord Stimulator: Current State and Future Directions" (2007).

<sup>27</sup> See Meloy, "Neurally Augmented Sexual Function" (2007).

<sup>28</sup> See Ansari et al., "Vagus Nerve Stimulation: Indications and Limitations" (2007).

<sup>29</sup> See Zhao et al., "EEG-Based Asynchronous BCI Control of a Car in 3D Virtual Reality Environments" (2009).

<sup>30</sup> See Principe & McFarland, "BMI/BCI Modeling and Signal Processing" (2008).

<sup>31</sup> See Ayaz et al., "Assessment of Cognitive Neural Correlates for a Functional Near Infrared-

strengths and weaknesses; for example, single-neuron recording is more invasive than EEG but less likely to be affected by artifacts from skin and muscle activity.<sup>32</sup>

### **BIDIRECTIONAL SENSORIMOTOR NEUROPROSTHETICS**

Bidirectional sensorimotor neuroprosthetics combine sensory and motor neuroprosthetics in a single device that both provides sense data to the device's human host and receives instructions from the human host that control the movement or other operation of the device. Some kinds of advanced prosthetic limbs are bidirectional sensorimotor neuroprosthetics: for example, an artificial hand may not only allow its human host to control the motion of the hand's fingers simply by willing such movements, but it may also provide the host with the ability to feel an object grasped within the hand and sense how much pressure is being generated from the hand's contact with the object.<sup>33</sup>

Although most contemporary virtual-reality video game systems do not satisfy the definition of "neuroprosthetics" offered here (insofar as they do not directly integrate with a player's neural circuitry), systems that allow a player to control his or her action in a virtual game-world by motions of his or her real-world body (e.g., registered using motion-detecting sensors) and which then provide immediate visual and auditory feedback through the VR headset about the way in which the player's action has changed the game-world offer an example of the kind of intense biocybernetic feedback cycle that can be generated using bidirectional sensorimotor technologies.<sup>34</sup>

### **COGNITIVE NEUROPROSTHETICS**

A cognitive neuroprosthetic device participates in or supplements processes that are internal to the mind of their human host and which do not directly involve either sensory or motor organs (although the processes may receive input from or transmit output to such organs). Such neuroprosthetic devices may participate in cognitive processes and phenomena such as

---

Based Brain Computer Interface System" (2009).

<sup>32</sup> See Miller & Ojemann, "A Simple, Spectral-Change Based, Electrographic Brain-Computer Interface" (2009).

<sup>33</sup> See Hoffmann, "Introduction to Neuroprosthetics" (2011), pp. 792-93.

<sup>34</sup> See Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics: Video Games as Tools for Posthuman 'Body Schema (Re)Engineering'" (2015).

memory,<sup>35</sup> imagination,<sup>36</sup> emotion,<sup>37</sup> belief, identity,<sup>38</sup> agency, attentiveness, consciousness,<sup>39</sup> and conscience.

The development of such technologies for use in human beings is still in its earliest stages. Although not the primary purpose for which the devices were designed, effects relating to creativity and one's sense of authenticity and agency have been reported in patients utilizing neuroprosthetic devices for deep brain stimulation.<sup>40</sup> Mnemoprosthetic devices that allow the creation or alteration of memories by manipulating the brain's natural mechanisms for the storage of memories have been experimentally tested in mice<sup>41</sup> and in principle could potentially be employed with the human brain, as well. However, such technologies currently fall far short of allowing the implantation of complex, content-rich memories into a mind or allowing the precise and detailed editing of existing memories.<sup>42</sup> Indeed, deep mysteries exist regarding the mechanisms by which long-term memories are created, stored, and retrieved in the human mind, and divergent theories have been proposed to explain the functioning of such systems.<sup>43</sup> As neuroscience continues to advance and competing theories are either confirmed or rejected, we will learn more about the kinds of cognitive neuroprosthetic devices that theoretically can or cannot be created and successfully integrated into the neural circuitry

---

<sup>35</sup> For the possibility of developing mnemoprosthetics, see Han et al., "Selective Erasure of a Fear Memory" (2009), and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).

<sup>36</sup> See Cosgrove, "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation" (2004), and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>37</sup> For the possibility of developing emotional neuroprosthetics, see Soussou & Berger, "Cognitive and Emotional Neuroprostheses" (2008); Hatfield et al., "Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior" (2009); Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>38</sup> See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011), and Berg, "Pieces of Me: On Identity and Information and Communications Technology Implants" (2012).

<sup>39</sup> For the possibility of neuroprosthetic devices relating to sleep, see Claussen & Hofmann, "Sleep, Neuroengineering and Dynamics" (2012), and Kourany, "Human enhancement: Making the debate more Productive" (2013), pp. 992-93.

<sup>40</sup> See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011).

<sup>41</sup> See Han et al., "Selective Erasure of a Fear Memory" (2009); Josselyn, "Continuing the Search for the Engram: Examining the Mechanism of Fear Memories" (2010); and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).

<sup>42</sup> For questions about the extent to which technological devices that directly store memories can ever become a part of the human mind, see Clowes, "The Cognitive Integration of E-Memory" (2013).

<sup>43</sup> See, for example, Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

and functioning of a human mind. (And conversely, the ability or inability to successfully develop and implement particular kinds of neuroprosthetic devices may shed light on whether particular proposed brain theories are correct or incorrect.) For example, if a model such as the Holonomic Brain Theory<sup>44</sup> were found to be correct, it could rule out the possibility of constructing neuroprosthetic devices that can create or alter a complex long-term memory simply by manipulating a modest number of neurons in a particular region of the brain.

### Neuroprosthetic devices categorized by purpose: therapy vs. enhancement

In addition to categorizing neuroprosthetic devices according to their function (i.e., as sensory, motor, bidirectional, or cognitive), such devices may also be categorized according to their purpose. For example, some neuroprosthetic devices are used for purposes of therapeutic **restoration**, to restore abilities that have been lost by a human being due to illness or injury. Other neuroprosthetic devices do not directly treat a medical condition but are instead used for purposes of **diagnosis**, to gather information about the condition of their human host and allow medical decisions to be made. Still other neuroprosthetic devices may be used for purposes of **identification**, to verify the identity of the device's human host, allow his or her whereabouts or activities to be tracked, or allow him or her access to some restricted area or resource.<sup>45</sup> Finally, some neuroprosthetic devices are designed for purposes of human **enhancement**: such devices augment, modify, or replace the sensory, motor, or cognitive abilities of their human host, allowing him or her to experience phenomena or perform actions that are not possible for the minds and bodies of natural, unmodified human beings.<sup>46</sup>

### Neuroprosthetic devices categorized by physical location: implant vs. prosthesis

---

<sup>44</sup> See Longuet-Higgins, "Holographic Model of Temporal Recall" (1968); Pribram, "Prolegomenon for a Holonomic Brain Theory" (1990); and Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web..." (1999).

<sup>45</sup> "Identification" has been used here in a loose sense; from the perspective of information security, what has just been described as "identification" actually involves identification, authentication, and authorization.

<sup>46</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 25.

Neuroprosthetic devices may alternatively be categorized according to their relationship with the body of their human host.<sup>47</sup> In this text, we use the word “**implant**” to describe a neuroprosthetic device that is surgically inserted into the body of its human host and which remains within the host’s body during the device’s operation.

Devices that are introduced into the body of their human host by nonsurgical means (such as nanorobots that are orally ingested) would not be “implants” in this sense, even if they establish a permanent connection with particular neurons after their entry into their host’s body; such technologies could be described more broadly as “**endosomatic**” devices or systems that are housed within their host’s body but are not surgically implanted. Neuroprosthetic devices formed of biological components that are grown or cultivated *in situ* within their host’s body would be another example of such endosomatic systems that are not, strictly speaking, implants.

Meanwhile, we can define a neuroprosthetic “**prosthesis**” as a device that is integrated into the neural circuitry of its human host but which is not completely contained within the host’s body but instead forms part of the exterior surface or boundary of the body and extends the body outward into the surrounding environment. It is possible for a single device to be both a neuroprosthetic implant and prosthesis: for example, an artificial eye that has been surgically implanted but which (at least, when the eyelid is open) forms part of the body’s exterior surface and a portion of its physical interface with the external environment. It is also possible for an implant and prosthesis to work together closely as part of a larger system. For example, an individual who has lost an arm due to injury may now possess a permanent implant located in the shoulder area that is integrated with the sensory and motor nerves that previously innervated the arm. If that implant contains an external socket that allows different robotic arms to be attached to it and controlled by the device’s host (or which perhaps even allows different kinds of robotic limbs and manipulators to be swapped in and out of the socket), then the socket itself would be considered an implant, and a robotic arm capable of connecting with the socket (and, through it, becoming indirectly integrated into the neural circuitry of the device’s human host) would be considered a prosthetic.

Note that some other texts that focus specifically on brain-computer interfaces (BCIs) may use terms such as “invasive,” “partially invasive,” and “noninvasive” to refer to a device’s physical relationship to the *brain* of its human host rather than its relationship to the host’s body as a whole. According to such definitions, a device could be wholly contained within the body of its human host but would be classified as “noninvasive” if it were implanted

---

<sup>47</sup> See Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012), p. 14.



in, say, the host's abdomen rather than the gray matter of his or her brain.<sup>48</sup> However, as defined in this text, a neuroprosthetic device must be integrated into the "neural circuitry" of its human host, but this does not necessarily require a connection to interneurons contained within the *brain*; a neuroprosthetic device could be located elsewhere in the body and possess a physical interface with afferent or efferent neurons. In the context of this book, "invasive" is best used to refer to neuroprosthetic devices that are endoscopic or fully contained within the human body of their host; "noninvasive" neuroprosthetic devices would be those that have no physical components contained within the body of their human host (such devices might include wearable neuroprosthetics that rest on the external surface of the body and which communicate with neurons via signals transmitted through the skin, or even devices that can communicate with neurons at a greater distance, through the generation and detection of electromagnetic fields or radiation); and "semi-invasive" neuroprosthetic devices would be those that have components that are external to (and perhaps not even physically connected to) their host's body but which simultaneously possess some components that must be introduced into the body of their human host (such as electronic components that must be inserted into the ear canal or through a permanent port installed in the body via a surgically created stoma, or biochemical agents that must be introduced into the host's bloodstream).

### Neuroprosthetic devices categorized by agency: active vs. passive

With regard to their interaction with the biological structures and processes of their human host, some neuroprosthetic devices may be considered "**active**," insofar as they possess an internal computer or other mechanism (e.g., a transmitter that allows the device to receive instructions from an external system) that governs the device's behavior and allows the device to proactively undertake actions and to determine how it will respond to stimuli received from the external environment or its human host. A "**passive**" neuroprosthetic device, on the other hand, is essentially an inert tool that lacks its own centralized internal control mechanism and whose behavior is controlled by the biological processes of and input supplied by the device's human host.<sup>49</sup>

---

<sup>48</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 14, and Panoulas et al., "Brain-Computer Interface (BCI): Types, Processing Perspectives and Applications" (2010).

<sup>49</sup> For one approach to classifying information and communications technology (ICT) implants as "active" or "passive" with regard for their functionality, see Roosendaal, "Implants and Human

An artificial eye that uses its built-in video camera to registers light from the external environment, utilizes its internal computer to process the incoming signals and convert them into a pattern of stimuli, and then stimulates retinal ganglion cells according to that pattern would be an active neuroprosthetic device; its internal computer governs its behavior, and if an adversary were able to access and compromise the computer, he or she could potentially use the device to supply its host with manipulated or even entirely fabricated visual data.<sup>50</sup>

On the other hand, an example of a passive implant would be an array of synthetic biomimetic physical neurons that is implanted into the host's brain to replace a group of natural biological neurons that had been destroyed through accident or energy. Although each individual synthetic neuron may possess a limited form of agency and control over its own actions – insofar as it possesses mechanisms that determine how it will react to particular stimuli – the device as a whole possesses no centralized control mechanism and is, in essence, an empty scaffolding that cannot fill itself with information or decide to take action. The natural biological neurons that are connected to the implant may eventually begin to “use” it by supplying stimuli to it and incorporating it into their network of activity and information storage, but such action cannot be forced or compelled by the implant itself.

#### **ATTACKS AGAINST ACTIVE VS. PASSIVE NEUROPROSTHETICS**

Note that if a neuroprosthetic device is controlled by an internal computer that possesses its own memory, processor, and input/output mechanisms and which runs its own operating system (and potentially additional specialized software), the device is almost certainly an “active” one, even if the intended purpose of the device is simply to detect the wishes and volitions of its human host and then to execute them. Although such a device may typically operate in a way that creates the *appearance* that it is strictly passive, an adversary who gained access to the device's computer and compromised its hardware or software could use the device as (or turn the device into) an active agent that behaves in ways that were not at all requested or desired by the device's human host. On the other hand, a purely passive neuroprosthetic devices could not be directly hijacked by an adversary and utilized to perform certain actions or behaviors, because the device itself has no internal control mechanism that can be hijacked; the only way that an adversary could indirectly dictate the actions of a passive neuroprosthetic device (without radically reengineering the device itself) would be to control the biological structures or processes of the device's human host that interact with the device, causing

---

Rights” (2012).

<sup>50</sup> Regarding such possibilities of neuroprosthetics being used to provide false data or information to their hosts or users, see McGee, “Bioelectronics and Implanted Devices” (2008), p. 221.

them to externally stimulate the device in ways that would produce a particular response.

### **Implantable computers vs. neuroprosthetic devices**

Not all implantable computers are neuroprosthetic devices: it is possible to have a miniaturized computer (e.g., as part of an active RFID transponder) that is implanted within a human being's body but which has no interface or interaction with the person's neural circuitry. Conversely, not every neuroprosthetic device is (or contains) an "implantable" computer: for example, a prosthetic arm may contain a highly sophisticated computer that is integrated into the neural circuitry of its human host through a stable physical connection and interaction with nerves in the person's shoulder, however the computer would be considered part of a "prosthesis" rather than an "implant."

### **Expected developments in neuroprosthetics: toward posthuman enhancement**

The kinds of neuroprosthetic devices that are currently in widespread use have typically been designed to serve a restorative or therapeutic medical purpose – for example, to treat a particular illness or restore some sensory, motor, or cognitive ability that their user has lost as a result of illness or injury. It is expected, though, that future generations of neuroprosthetics will increasingly be designed not to restore some ordinary human capacity that is absent but to enhance their user's physical or intellectual capacities by providing abilities that exceed or differ from what is naturally possible for human beings.<sup>51</sup> The potential use of such technologies for physical and cognitive enhancement is expected to expand the market for neuroprosthetics and implantable computers to reach new audiences well beyond the limited segment of the population that currently relies on them to treat medical conditions.<sup>52</sup>

Researchers expect that future versions of sensory neuroprosthetics such as retinal implants may give human beings the capacity to experience their environments in dramatically new ways, for example through the use of telescopic or night vision<sup>53</sup> or by using a form of augmented reality that overlays

---

<sup>51</sup> See Gasson, "ICT implants" (2008); Gasson et al., "Human ICT Implants: From Invasive to Pervasive" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); and Merkel et al., "Central Neural Prostheses" (2007).

<sup>52</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), and Gasson et al., "Human ICT Implants: From Invasive to Pervasive" (2012).

<sup>53</sup> See Gasson et al., "Human ICT Implants: From Invasive to Pervasive" (2012), and Merkel et al.,

actual sense data provided by the environment with supplemental information received or generated by a neuroprosthetic device's computer.<sup>54</sup> Some researchers envision the development of devices that resemble more sophisticated forms of retinal and cochlear implants that can record all of a person's audiovisual experiences for later playback on demand, effectively granting the person perfect audiovisual memory<sup>55</sup> and potentially allowing the individual to share his or her sensory experiences with others (e.g., through automatic upload to a streaming website).

Building on successful experiments with implanting artificial memories in mice,<sup>56</sup> other researchers have envisioned the possibility of a person being able to regularly download new content onto a memory chip implanted in his or her brain, thereby instantaneously gaining access to new knowledge or skills.<sup>57</sup> Even more futuristic scenarios envisioned by scholars include the development of a "knowledge pill" that can be ingested and whose contents – perhaps a swarm of web-enabled nanorobots<sup>58</sup> – travel to the brain, where they modify or stimulate neurons to create engrams containing particular memories.<sup>59</sup> Another potentially revolutionary technological advancement is the ongoing development of brain-machine-brain interfaces<sup>60</sup> that may eventually allow direct and instantaneous communication between two human brains physically located thousands of miles apart.

---

"Central Neural Prostheses" (2007).

<sup>54</sup> See Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012).

<sup>55</sup> See Merkel et al., "Central Neural Prostheses" (2007), and Robinett, "The consequences of fully understanding the brain" (2002).

<sup>56</sup> See Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).

<sup>57</sup> See McGee, "Bioelectronics and Implanted Devices" (2008).

<sup>58</sup> See Pearce, "The Biointelligence Explosion" (2012).

<sup>59</sup> See Spohrer, "NBICS (Nano-Bio-Info-Cogno-Socio) Convergence to Improve Human Performance: Opportunities and Challenges" (2002).

<sup>60</sup> See Rao et al., "A direct brain-to-brain interface in humans" 2014. Existing experimental technologies of this sort are sometimes described as "brain-brain interfaces" (BBIs), although we would argue that such terminology is somewhat inaccurate and misleading; it would be more appropriate to describe the system as a "brain-machine-brain interface" (BMBI) or "brain-computer-brain-interface" (BCBI). If one were allowed to describe as a "brain-brain interface" a system that actually interposes between the two brains some complex technological device that enables and mediates their communication, then traditional technologies such as telephones and even books could similarly be described as "brain-brain interfaces" with just as much legitimacy. We would argue that a true "brain-brain interface" would instead be one in which the communication between the two brains does not rely on any "external" device or system; rather, the means of communication between the two brains would be contained within and fully integrated into one or both of the brains themselves. An electronic transmitter that is permanently implanted within a host's brain and which harvests energy from the brain itself and allows the brain to communicate with other brains possessing similar devices could arguably be described

## Early adopters of neuroprosthetic devices for posthuman enhancement

One group of potential “early adopters” of neuroprosthetic devices designed for human enhancement includes military forces, intelligence agencies, police forces, and other government agencies that may use such technologies to enhance the capacities of their personnel to engage in conventional combat operations, cyberwarfare, and the gathering and analysis of intelligence.<sup>61</sup> Another potential group of early adopters of such technologies includes hardcore computer gamers (including professional competitive gamers) who wish to experience more sophisticated and immersive forms of sensorimotor interaction with game-worlds and cybernetic interaction with their fellow gamers than can be provided by external virtual reality systems.

## Neuroprosthetic devices categorized by cybernetic characteristics: reality, virtuality, xenosomatics, and hive minds

In addition to using functional and teleological classification schemes as previously described, neuroprosthetic devices can also be classified according to the cybernetic relationships of communication and control that they create or support between the mind of a device’s host, his or her body, and some real or virtual external environment. Such classification schemes will become especially important when considering future posthuman neuroprosthetic devices and systems that are able to grant their hosts or users unusual new types of capacities. For example, a neuroprosthetic device might aid its human host to sense and manipulate a real physical environment using his or her natural physical body; supply a new physical body for use in sensing and manipulating a real physical environment; aid the human host to sense and

---

as a “brain-brain interface.” A clearer example would be that of a prosthetic composed of biological material that is either implanted into or grown or assembled within a brain, and which through its unique organic design is capable of generating and detecting radio frequency transmissions, light, electromagnetic fields, ultrasonic waves, or other phenomena that are detectable at a distance. If two brains possessing such prosthetics were able to communicate with one another by means of the devices, this could well be understood as an example of a “brain-brain interface,” even if the devices in fact were reliant on a medium (such as that of the atmosphere) for transmission of their signals. In its functioning, such a system would approach traditional definitions of “telepathy.”

<sup>61</sup> On potential military use of neuroprosthetic devices, see Schermer, “The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction” (2009), and Brunner & Schalk, “Brain-Computer Interaction” (2009).

manipulate a virtual environment using his or her human (or at least, a human-like) body; or provide the host with a radically nonhuman body for use in sensing and manipulating a virtual environment.<sup>62</sup>

In this context it is preferable not to contrast “physical” and “virtual” environments, because even “virtual” environments created through virtual reality headsets or direct stimulation of a person’s brain are eminently “physical,” insofar as they exist as information stored on physical memory devices and require the carefully arranged transmission of chemicals or electrons in order to physically alter receptor cells or neurons in the brain. A better distinction would be between “virtual” environments whose form of actual physical existence (e.g., as patterns of magnetization in the ferromagnetic layer of a hard disk drive’s platter) does not directly provide or reflect the environment that a human being experiences and manipulates through his or her sensory, cognitive, and motor action, on the one hand, and “real” or “analogue” environments, on the other hand, whose form of actual physical existence directly provides, informs, and corresponds to the form of the environment as it is sensed and manipulated by a human being who is experiencing it.<sup>63</sup>

An appendix to this text presents a cybernetic classification of neuroprosthetic devices that encompasses devices ranging from those whose cybernetic characteristics are similar to those of conventional tools and technological devices (such as automobiles or smartphones) to those whose cybernetic characteristics are so revolutionary and transformative as to be potentially “posthuman.” The latter might include, for example, a xenosomatic device that provides its human host with “the experience of a new body that is radically *nonhuman*,”<sup>64</sup> a neosomatic device that “physically replaces the entire body apart from the brain (i.e., creates a full-body cyborg),”<sup>65</sup> and syzygocybernetic devices that introduce into their user’s mind some external agency in such a way that the device’s hostmind is aware of and experiences the other agent’s or agents’ mental activity from within the hostmind’s own cognitive processes, rather than simply as sensory input; such devices could potentially link the conscious awareness of multiple human hosts to allow for the creation of “hive minds” and communal thought.<sup>66</sup>

---

<sup>62</sup> See Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics...” (2015).

<sup>63</sup> According to this definition, dream-worlds that are encountered during sleep would also be considered “virtual” rather than “real.”

<sup>64</sup> See Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics...” (2015).

<sup>65</sup> See Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics...” (2015).

<sup>66</sup> See Gladden, “Tachikomatic Domains: Utopian Cyberspace as a ‘Contingent Heaven’ for Humans, Robots, and Hybrid Intelligences” (2015), and Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics...” (2015).

## The meaning of “advanced” neuroprosthetics

This text addresses the needs and practices of ensuring information security for advanced neuroprosthetics. By “advanced,” we mean that this book considers all types of neuroprosthetic devices whose future development is anticipated, and not simply those kinds that already are in widespread use among human beings (such as cochlear implants), are approved for experimental therapeutic use in human beings (such as certain kinds of artificial retinas with a quite limited visual resolution), or which are currently being tested in animals but could potentially be adapted someday for use in human beings (such as some kinds of mnemoprosthetics designed to create or alter particular memories<sup>67</sup>).

Many of the IMDs that are currently in use around the world – especially those that were implanted years or even decades ago – represent both a blessing and a unique challenge from the perspective of information security, insofar as their internal computers are severely constrained in their capacities and functionality; this may prevent one from applying conventional information security mechanisms and software that are commonly employed with more powerful computers (e.g., those found in desktop computers or smartphones) while simultaneously shielding the devices from attacks to which only more powerful conventional computers and operating system may be vulnerable. Looking ahead to the future, though, we can anticipate the need to provide information security to implanted neuroprosthetic devices that differ radically from today’s best desktop computers not by being so much less powerful and sophisticated than they are, but by being so much *more* so – or, indeed, by utilizing exotic hardware and software platforms (such as biomolecular computing) that have little in common with today’s computers designed for general office or home use.

While this text considers all such devices that are currently in widespread use or are undergoing testing, the scope of the book is broader: it also addresses the information security needs of those more advanced kinds of neuroprosthetic devices (such as artificial retinas with much higher visual resolution) that scientists, engineers, and entrepreneurs have declared their intention to create and are actively working to bring to market, as well as more sophisticated neuroprosthetic devices whose eventual development is expected by scientists, engineers, and professional futurists and whose social, cultural, political, legal, ethical, economic, and technological implications are

---

<sup>67</sup> See Han et al., “Selective Erasure of a Fear Memory” (2009) and Ramirez et al., “Creating a False Memory in the Hippocampus” (2013).

already being debated by the proponents and critics of particular technologies.

Among such potential future neuroprosthetic technologies are many kinds of devices and systems – such as those allowing human beings to acquire new sensory capacities,<sup>68</sup> adopt radically nonhuman bodies,<sup>69</sup> inhabit virtual worlds in which different laws of physics and biology hold sway,<sup>70</sup> and directly link their minds with one another or with artificial intelligences to create new kinds of communal thought and agency.<sup>71</sup> Although today there is not yet a widespread practical necessity to *implement* information security mechanisms and procedures for such systems, it is important to begin developing the theoretical, conceptual, and organizational frameworks that will be needed to promote the information security of systems utilizing such technologies – especially insofar as the formulation of sound information security frameworks can aid those individuals and organizations that are actively pursuing the development of such technologies, to help ensure that they are designed and eventually deployed in ways that will advance rather than undermine essential aims such as human authenticity, agency, and full human development.<sup>72</sup>

---

<sup>68</sup> See Merkel et al., “Central Neural Prostheses” (2007).

<sup>69</sup> See Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics...” (2015).

<sup>70</sup> See Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics...” (2015).

<sup>71</sup> Gladden, “‘Upgrading’ the Human Entity...” (2015).

<sup>72</sup> See Gladden, “Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems” (2015), and Gladden, “‘Upgrading’ the Human Entity...” (2015).





## Chapter Two

# An Introduction to Information Security in the Context of Advanced Neuroprosthetics

### Institutional processes and personal practices

Information security (also known as InfoSec) has been defined as “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.”<sup>1</sup> The work of attempting to provide such protection is a never-ending process; information security is not a static state that can be achieved once and for all but is rather a goal to be pursued. While large organizations are able to implement sophisticated information security plans that are developed and executed by dedicated specialists, even individual consumers and users of information technology instinctively utilize many information security practices in an effort to keep sensitive information private and secure. In this chapter we briefly describe some of the foundational concepts of information security that will be explored in greater depth throughout this book.

### The CIA Triad

A key principle of information security is that of ensuring the **confidentiality, integrity, and availability** of information for authorized use by authorized users. The original “CIA Triad” of information security objectives<sup>2</sup> has been expanded by various researchers and practitioners through the addition of other proposed objectives,<sup>3</sup> but it remains the most concise and universally recognized summary of the goals that the field of information security seeks

---

<sup>1</sup> 44 U.S.C., Sec. 3542, cited in *NIST SP 800-53*, Rev. 4 (2013), p. B-10.

<sup>2</sup> Rao & Nayak, *The InfoSec Handbook* (2014), pp. 49-53.

<sup>3</sup> See Parker, “Toward a New Framework for Information Security” (2002), and Parker, “Our Excessively Simplistic Information Security Model and How to Fix It” (2008).

to achieve. We will consider the relationship of the CIA Triad and other information security objectives to neuroprosthetic devices in detail in Chapter Five.

It is essential to note that as it relates to advanced neuroprosthetic devices, information security is not only concerned with maintaining the confidentiality, integrity, and availability of information contained within a neuroprosthetic device itself (e.g., proprietary software used to control the device). Insofar as a neuroprosthetic device is linked to the neural circuitry of its human host, an adversary who gains unauthorized access to the device could compromise the confidentiality of information relating to the internal biological processes and medical status of its human host – and could potentially even detect the contents of cognitive processes such as thoughts, fears, imaginings, emotions, memories, and beliefs. Moreover, the integrity and availability of information stored or existing within the mind of a human host could also be at risk, if an adversary could use a neuroprosthetic device to alter, manipulate, or damage the biological structures, biochemical and bioelectrical activity, and patterns of information stored within the host's network of neurons.<sup>4</sup> The designers and operators of neuroprosthetic systems must also take into account the fact that a device such as an artificial eye could conceivably be illicitly accessed by an adversary not to gather information about the host in whose body the device is implanted but about some unrelated party who is the actual target of the adversary's unauthorized surveillance and who only coincidentally happens to be standing near the device's host at the moment. Thus the presence of advanced neuroprosthetic devices within a human society can potentially impact the confidentiality, integrity, and availability of information for individuals beyond the limited number of persons who personally possess such devices.

## Security controls

One of the primary means of protecting information is to design and implement effective **security controls**. A security control can be understood as “A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.”<sup>5</sup> Such controls can be either **administrative** (i.e., consisting of organizational policies and procedures), **physical** (i.e., created by physical walls and barriers, motion-

---

<sup>4</sup> See Gladden, “‘Upgrading’ the Human Entity...” (2015), and Merkel et al., “Central Neural Prostheses” (2007).

<sup>5</sup> *NIST SP 800-53*, Rev. 4 (2013), p. B-21.

detecting alarm systems, electric fences, security guards, or the physical isolation of a computer from any wired network connections), or **logical** (i.e., enforced through software or other electronic or computerized decision-making).<sup>6</sup> Together, administrative and physical controls can be understood as “non-computing security methods,” which “are security safeguards which do not use the hardware, software, and firmware of the IT.”<sup>7</sup>

### An example of administrative, logical, and physical controls

Consider, for a moment, an advanced cochlear implant that not only presents its human host with high-fidelity live audio received from the external environment but which also: 1) records all of the auditory data that it receives to an internal memory card that the device’s host can access at any time through an act of will to “play back” previous auditory experiences, and 2) wirelessly transmits a live stream of the recorded audio to a cloud-based storage system to create a permanent external backup of all the host’s auditory experiences.

Such a device would gather – and have the potential to gather – vast and diverse quantities of data relating to the device’s human host, other human beings or technological systems that interact with the host, and other human beings or systems that simply happen to be near the host. The device would likely record not only all of the host’s personal and professional conversations (as well as all of the other conversations taking place in, say, a crowded restaurant in which the host was dining), but also all of the auditory contents of all the music, films, theatrical performances, and computer games that the host experiences, as well as the sound of the host’s heartbeat and breathing (which can be used to infer details about his or her physical activities and health status).

In the case of such a device, examples of physical controls might include designing, constructing, and implanting the device in such a way that it has no external ports or sockets that are accessible from the exterior of its host’s body (and which adversaries could potentially illicitly access) or adding a tamper-proof seal that prevents physical access to the device’s internal components. Within an organizational setting, physical controls might also include soundproofed walls and secured doors that prevent individuals who possess such devices from entering parts of the building in which the devices could be illicitly used to record sensitive conversations.

Logical (or “technical”) controls are those grounded in the ability of software to analyze decisions and take particular actions according to specified rules. For example, the advanced cochlear implant’s internal computer might

---

<sup>6</sup> Rao & Nayak, *The InfoSec Handbook* (2014), pp. 66-69.

<sup>7</sup> NIST SP 800-33 (2001), p. 21.

be programmed with filters that prevent the recording of sounds of particular volumes and frequencies (e.g., to block the recording of its owner's heartbeat) or even to identify and prevent the recording and playback of particular kinds of sounds (e.g., commercially released music) representing intellectual property whose use is legally restricted. The device may also use logical controls to allow its human host and authorized maintenance or medical personnel to wirelessly log into the device's command console and reconfigure its settings while blocking unauthorized users from gaining such access. An organization may also deploy software within the ubiquitous computing environment of its R&D facility that detects the presence of visitors who possess such advanced cochlear implants and broadcasts white noise in targeted locations to prevent such devices from recording sensitive conversations among the facility's staff. While the sound waves of the white noise itself might constitute a physical control, the software that analyzes data to determine the presence of visitors within the building and decides whether, when, and how to broadcast such sounds would constitute a logical control (which could potentially be disabled or evaded through logical means).

Administrative controls are those grounded in policies and procedures that are designed to be carried out by human beings.<sup>8</sup> The extent to which they are successfully enforced depends on many factors, including the competence, commitment, training, and motivations of the individuals charged with enforcing them. In the case of our advanced cochlear implant, a user of the device might develop his or her own personal administrative controls or policies relating to its use. For example, perhaps the person has decided that he or she will always disable the device's recording function (while still allowing himself or herself, however, to experience a live stream of the auditory

---

<sup>8</sup> Although there may be circumstances in which an artificial agent or system participates in the enforcement of administrative controls, the role of such a software-based technological system can often be better understood as constituting a logical rather than administrative control. It could be appropriate to speak of an artificial system as managing the implementation of administrative controls in a human-like sense if the system possessed a kind and degree of artificial intelligence (e.g., produced by an advanced physical neural network) such that its behaviors were not strictly determined by the code contained in a particular computer program but instead resulted from the system's application of its own reasoning, memories, imagination, values, conscience, and judgment to arrive at decisions that are not necessarily entirely predictable. Such an artificially intelligent system would – like human beings – be capable of either strictly enforcing administrative controls, allowing periodic (and unauthorized) exceptions to the administrative controls on the basis of the agent's own values and personal experience, shirking one's responsibilities and failing to enforce administrative controls out of laziness or resentment, failing to enforce administrative controls because they were not properly understood, or periodically failing to enforce administrative particular controls because – in the agent's best judgment – resources or attention needed to be allocated to other, more important priorities, instead.

data received by the device) whenever engaging in certain kinds of sensitive conversations with particular individuals or while asleep during the night. The company that designs and manufactures the device, meanwhile, might develop its own policies and procedures that determine how different kinds of authorized maintenance and emergency medical personnel around the world can apply for and receive a special kind of certification and an access code that allows them to log into the command console of any such device.<sup>9</sup> Insofar as it is legally and ethically permissible, an organization may also develop policies that require all of its employees who possess or acquire such an advanced cochlear implant to notify the organization of this fact and to follow specified practices that restrict them from entering certain areas of the organization's facility in which they could purposefully or unintentionally record auditory data containing highly sensitive organizational information.

We will consider the use of such administrative, logical, and physical controls to provide information security for neuroprosthetic devices and systems in greater detail in Chapters Seven, Eight, and Nine.

## Overlap of different kinds of security controls

In principle, it should be possible to categorize security control systems according to whether they fill a role of authentication or authorization or whether they are administrative, logical, or physical. In practice, though, there is significant overlap among categories. For example, a company's server might be protected inside a dedicated server room whose door is secured with a tumbler lock that requires a traditional physical key to open. The fact that a user must possess a physical key in order to open the door makes this system a physical access control. However, if, for example, the company has effective policies and procedures in place to govern the possession and use of the key (e.g., only two members of the IT staff have a copy of the key, or the key is stored in a safe in a different part of the company's facility and can only be temporarily checked out by IT personnel when needed), then it is also part of an administrative control system. Moreover, if the physical key also contains an embedded RFID chip that must be detected by the lock's electronic RFID reader before the lock will open (in order to prevent unauthorized copies of the key from opening the lock), then the key would also be part of a logical access control system. In addition, the key not only serves a purpose of authenticating its user (since presumably only one of the server room's intended users would have a copy of the key), but it also serves the purpose of authorization by allowing the authenticated user to open the

---

<sup>9</sup> For a discussion of such certificate schemes for implantable medical devices, see, for example, Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), and Freudenthal et al., "Practical techniques for limiting disclosure of RF-equipped medical devices" (2007).

door, enter the room, and access the resources inside, while the lack of a key prevents unauthenticated parties from entering the room.

Similarly, a closed-circuit TV camera that monitors the hallway leading to the server room is a physical control, insofar as it creates a physical obstacle that an unauthorized party seeking access to the server room might try to avoid. If the live video is being processed by a software program that continually scans the images and alerts a human security staff member when particular phenomena are detected in the video (e.g., the images of a human being approaching the server room door), this would constitute a logical control. Finally, if the human security staff member – upon seeing the live video of someone approaching the server room door – follows a particular set of guidelines to decide whether he or she should go and investigate the situation or simply ignore it, this would be an administrative control.

## Authentication and authorization

In order to assure that information is readily available for use by its intended users but not available to any other parties, there must be some system or mechanisms in place that can either block or unlock access to the information, depending on the circumstances of who is seeking the information and for what purpose. Access controls are systems or mechanisms of this sort that are designed to “Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.”<sup>10</sup> Rao and Nayak note that such access controls are “considered the most important aspect of information security.”<sup>11</sup>

An access control must perform two key functions.<sup>12</sup> First, it carries out the step of **authentication**, or verifying the identity of the entity that is attempting to access the protected information – whether that entity be a human being, device, or software process.<sup>13</sup> Second, the access control carries out the step of **authorization**, or granting the user access to those portions of the information system and the information contained within it that the user is authorized to access<sup>14</sup> (which, in the case of unauthorized users, may be no information at all).

---

<sup>10</sup> NIST SP 800-33 (2001), p. 20.

<sup>11</sup> Rao & Nayak, *The InfoSec Handbook* (2014), p. 63.

<sup>12</sup> Rao & Nayak, *The InfoSec Handbook* (2014), p. 63.

<sup>13</sup> NIST SP 800-33 (2001), p. 20.

<sup>14</sup> Rao & Nayak, *The InfoSec Handbook* (2014), pp. 62-76.

## Vulnerabilities, threats, and risks

Within the field of information security, words such as “vulnerability,” “threat,” and “risk” are often employed to convey specific technical meanings.<sup>15</sup>

A **vulnerability**, for example, can be understood as “A weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system’s security policy.”<sup>16</sup> In the case of neuroprosthetic devices, we might say that a robotic prosthetic arm displays a significant vulnerability if it possesses an exposed USB port that can be used to access the device’s internal computer. Similarly, an artificial eye displays a vulnerability if a beam of light directed at the eye with a particular frequency and intensity will automatically cause the artificial eye’s internal computer to reboot.<sup>17</sup> Note that while such characteristics might be considered “vulnerabilities” from the perspective of information security, from a functional and operational perspective they might simultaneously be considered essential features that are necessary to ensuring the effective functioning of the device and thus the health and well-being of its human host.

In themselves, the vulnerabilities displayed by a neuroprosthetic device do not cause a loss of information security for the device’s host or operator; such harm results only when a particular **threat source** interacts with the device in such a way which – because of the existence of the vulnerability – compromises the confidentiality, integrity, or availability of information. A threat source may be an agent such as a human adversary or computer virus that purposefully targets and exploits the vulnerability (in which case the threat-source’s action can be considered an “attack”), or a threat source could be some unintentional and purely accidental occurrence within a neuroprosthetic device, its human host, or the surrounding environment that triggers

---

<sup>15</sup> Throughout this text other words such as “danger” and “hazard” may sometimes be used; these terms are employed more generally and without a specific technical meaning. Depending on the context, they may refer to something that is a vulnerability, threat source, threat, risk, or some combination of these.

<sup>16</sup> *NIST SP 800-33* (2001), p. 18.

<sup>17</sup> Hansen and Hansen raise the hypothetical situation of a poorly designed prosthetic eye whose internal computer can be disabled if the eye is presented with a particular pattern of flashing lights; see Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010). In the example that we present here, the behavior of our hypothesized artificial eye is not a bug or flaw that results from poor design (and perhaps has not yet even been discovered by the device’s designer or users) but rather a feature that has been intentionally added by the device’s designer, e.g., to facilitate diagnostic, maintenance, or emergency control activities that may periodically need to be performed by maintenance or medical personnel.



the effects of the vulnerability.<sup>18</sup> In the case of the robotic prosthetic arm displaying the vulnerability of an exposed USB port, a threat source could be a human adversary with a USB flash drive containing malicious code that will hijack control of the arm and cause it to behave in a particular way after the flash drive is plugged into the port.<sup>19</sup> In the case of the artificial eye that automatically reboots when exposed to a particular frequency and intensity of light, a threat source could be a computer monitor on which a movie is being played that causes light of various frequencies and intensities to be emitted from the screen.

Similarly, we can understand a **threat** as the possibility that some threat source will either intentionally attempt to exploit (as in the case of a cyberattack) a vulnerability or will unintentionally trigger (as in the case of some random environmental phenomenon) the vulnerability's effects.<sup>20</sup> In the case of the robotic prosthetic arm, a threat exists if there are adversarial agents in the environment attempting to exploit the device's vulnerability, or if there is a possibility that such threat sources may exist, or if other threat sources exist (such as USB flash drives containing executable code that is not intentionally malicious but which – if inserted into the device's USB port – would cause the device's internal computer to crash). In the case of the artificial eye, a threat exists if there are (or, as far as one knows, may be) light sources of the relevant frequency and intensity in areas that the device's human host might enter.

With regard to an advanced neuroprosthetic device, the **risk** arising from a particular vulnerability and set of threats is an impact borne by the device's human host, operator, and other individuals or organizations responsible for the device's development and use.<sup>21</sup> The risk is influenced by the probability that a threat source will intentionally attack the device's vulnerability or unintentionally trigger its effects as well as by the nature and extent of the harm that would occur as a result.

Best practice in the field of information security requires individuals and organizations to proactively address the risks that they face, which is done by

---

<sup>18</sup> NIST SP 800-33 (2001), p. 18. In the case of implantable medical devices, the "compromised vulnerability" through which a threat acts is also known as the "threat vector" or "etiological agent;" see Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

<sup>19</sup> For the possibility of an adversary gaining control of a prosthetic limb, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

<sup>20</sup> NIST SP 800-33 (2001), p. 18.

<sup>21</sup> NIST SP 800-33 (2001), p. 18.

developing and implementing a program of **risk management**.<sup>22</sup> The first step in such a program is to determine the scope, nature, and context of the activities to be considered.<sup>23</sup> In the case of an organization that designs and manufactures neuroprosthetic devices, it may focus on the need to provide information security for the sensitive and valuable proprietary research and design data developed by its laboratories and engineers during the R&D stage as well as building into the devices basic systems to protect the information security of their end users. Meanwhile, an individual user who has purchased a neuroprosthetic device as a consumer electronics device will presumably not have the desire or resources to monitor whether the device's manufacturer is able to keep confidential its internal research data; instead, he or she may focus on the information security risks arising from the device's intended use of the device in a very specific situation (e.g., to enhance his or her workplace performance or treat the symptoms of a particular neurological condition). Having determined the risk context, an individual or organization then conducts a **risk assessment** to identify specific vulnerabilities, threat sources, threats, and risks that are relevant, given the chosen risk context.<sup>24</sup>

Each individual and organization must determine how much risk it is willing to bear, taking all relevant elements into consideration. In some cases, **risk mitigation** can be employed to reduce the risk associated with a neuroprosthetic device to a level that the individuals or organizations involved find acceptable. Risk mitigation attempts to reduce a risk and its impact by seeking to either eliminate a vulnerability at its source, add protections that prevent the vulnerability from being intentionally exploited or accidentally triggered, or reduce and contain the harm that will result from exploitation or triggering of the vulnerability.<sup>25</sup> In the case of the robotic prosthetic arm described above, risk mitigation might involve removing or disabling the USB port, adding a cosmetic cover that conceals its existence, or installing security software that automatically scans a flash drive upon its insertion and prevents the execution of any programs or code contained on it. In the case of the artificial eye, risk mitigation might include wearing sunglasses that block light of a particular frequency or simply informing the device's human host about the vulnerability and providing instructions on how to best react if the device should accidentally encounter light of the relevant color and brightness and automatically reboot itself.

---

<sup>22</sup> NIST SP 800-33 (2001), p. 19.

<sup>23</sup> NIST SP 800-33 (2001), p. 19.

<sup>24</sup> NIST SP 800-33 (2001), p. 19.

<sup>25</sup> NIST SP 800-33 (2001), p. 19.

In some cases, risk mitigation may not be able to reduce the risk associated with a particular neuroprosthetic device to a level that the individuals or organizations involved consider acceptable; in those circumstances, the decision may be made to simply not use such a device.

## Classifying vulnerabilities, threat sources, and threats

Researchers have proposed a number of ways of describing and categorizing vulnerabilities, threats, and risks relating to implantable medical devices (IMDs); many of these proposed classification schemes may also be relevant for advanced neuroprosthetic devices. Below we consider several of these classification schemes.

### VULNERABILITY MODELS

Hansen and Hansen propose a model for identifying and categorizing both the conditions that are required in order for a particular vulnerability to exist for IMDs and the effects that can occur as a result of the vulnerability being triggered or exploited.

- **Classifying the preconditions for vulnerabilities.** In Hansen and Hansen's model, the "etiology" or unique set of circumstances in which a particular vulnerability can be exploited or triggered can be described with reference to three factors: the degree of **physical proximity** to the implanted device that a particular threat source must possess in order for the vulnerability to be triggered or exploited; particular **device activity** that the implanted device must be carrying out (typically, either "sensing," "actuating," "information processing," or "communicating") in order for the vulnerability to exist; and any particular **state of the device's host** (such as a certain body position or posture, heart rate, state of conscious awareness, movement, or other activity) that must exist in order for the vulnerability to be triggered or exploited.<sup>26</sup>
- **Classifying the effects of compromised vulnerabilities.** In Hansen and Hansen's model, the impacts or "pathogenesis" of vulnerabilities within IMDs that have been triggered or exploited can be described with reference to two factors: the **component affected** (which can be either the implanted medical device, an external system that interacts with the implanted device, or the biological organism of the device's host) and the permanence of the impact (which might, for example, dissipate after a short time on its own, even without any intervention or attempt to address the impact; create a change in the implanted

---

<sup>26</sup> See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

device, external system, or host's biological organism that will remain until it is proactively addressed and treated; or remain permanently without the possibility of being counteracted, treated, or removed).<sup>27</sup>

### THREAT SOURCE MODELS

In discussing security for IMDs, Halperin et al. present the following types of adversaries, while acknowledging that other types may be possible:

- **Passive adversaries** are those that “eavesdrop on signals (both intentional and side-channel) transmitted by the IMD and by other entities communicating with the IMD.”<sup>28</sup>
- **Active adversaries** are those which in addition to simply eavesdropping “can also interfere with legitimate communications and initiate malicious communications with IMDs and external equipment.”<sup>29</sup>
- **Coordinated adversaries** are multiple adversaries who “coordinate their activities—for example, one adversary would be near a patient and another near a legitimate IMD programmer.”<sup>30</sup>
- **Insiders** who may constitute a threat source can include “healthcare professionals, software developers, hardware engineers, and, in some cases, patients themselves”<sup>31</sup> who have the desire and ability to launch an intentional attack or who have the capability of unintentionally triggering a vulnerability and its effects.

Halperin et al. also note that adversaries can also be distinguished based on whether they use “**standard equipment**” (such as a legitimate “device programmer” unit that is produced by the manufacturer of an IMD and intended for use by authorized medical personnel in monitoring, updating, reconfiguring, or controlling the IMD) or “**custom equipment**” (which may include homemade surveillance or control devices whose nature or capacities render the devices illegal).<sup>32</sup>

### THREAT AND ATTACK MODELS

#### *Passive vs. active attacks*

Cho and Lee classify potential threats as either passive or active attacks on implanted biosensors. In their framework:

<sup>27</sup> See Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010).

<sup>28</sup> See Halperin et al., “Security and privacy for implantable medical devices” (2008), p. 35.

<sup>29</sup> See Halperin et al., “Security and privacy for implantable medical devices” (2008), p. 35.

<sup>30</sup> See Halperin et al., “Security and privacy for implantable medical devices” (2008), p. 35.

<sup>31</sup> See Halperin et al., “Security and privacy for implantable medical devices” (2008), p. 35.

<sup>32</sup> See Halperin et al., “Security and privacy for implantable medical devices” (2008), p. 35.

- **Passive attacks** are those in which an adversary can “eavesdrop and collect the exchanged messages between a central device and each biosensor,” however the adversary “cannot inject and modify an payload to the central device” and has “no ability to make a physical attack” to the implanted device; geolocating a device’s host by eavesdropping on the device’s transmissions would be a form of passive attack.<sup>33</sup>
- **Active attacks** on an implanted biosensor are those that incorporate “injecting/ modifying/blocking payload as well as eavesdropping;” they include denial of service attacks and spoofing attacks that may allow an adversary to impersonate other devices in their communication with the biosensor (or impersonate the biosensor in its communication with other devices).<sup>34</sup>

Cho and Lee suggest that the range of possible active attacks on an implanted biosensor does not include attacks involving direct physical access to the biosensor, as gaining physical access to such an implanted biosensor would be “impossible.”<sup>35</sup> While such attacks might admittedly be complex and difficult (and, in many cases, undesirable for adversaries), we would contend that it is naïve to exclude the possibility of an active attack that does involve an adversary gaining physical access to an implanted device: it is undoubtedly true that many adversaries who have the desire and ability to remotely attack an individual’s implant through wireless transmissions would have neither the desire nor ability to physically assault and mutilate the individual in order to gain direct physical access to his or her implanted device. However, the possibility cannot be ruled out; moreover, with future advances in nanotechnology and other technologies, it may someday become possible, for example, for an adversary to gain direct physical access to another person’s implanted device not by performing a surgical operation but simply by spiking the person’s beverage with an undetectable nanorobot cloud which, after ingestion, will travel through the person’s body to the device.

#### ***Eavesdropping, impersonation, and jamming attacks***

Ankarali et al. take a different approach in classifying attacks on implantable medical devices. They categorize malicious attacks on IMDs into three

---

<sup>33</sup> See Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012), p. 208.

<sup>34</sup> See Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012), p. 208.

<sup>35</sup> Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012), p. 208.

categories: eavesdropping, impersonation, and jamming attacks. In their model:

- **Eavesdropping** attacks are those that “compromise the secrecy of transmitted private data e.g., patients’ personal information, medical measurements, user location, and information that may be used to perform additional attacks [...]”<sup>36</sup>
- **Impersonation** is an attack in which an adversary impersonates an authorized user or system and is erroneously authenticated by an IMD. An adversary who has successfully impersonated an authorized user could potentially install malware on the IMD, steal information stored within it, cause it to behave in a way that would quickly exhaust its battery, or directly affect the host’s organism in a way that could potentially be harmful or fatal.<sup>37</sup>
- **Jamming** is an attack in which an adversary undertakes a denial of service attack “by flooding the operating frequency of medical devices with an irrelevant signal,” which can make it very difficult for a targeted IMD to carry out communication with external systems or other implanted devices that may be necessary for the IMD’s successful functioning.<sup>38</sup>

#### *Electronic, biological, psychological, or hybrid attacks*

The threat models described above deal with attacks that are launched against neuroprosthetic devices in their nature as electronic devices. We would note, however, that such narrow, electronically focused models are inadequate to capture the full range of threats relating to neuroprosthetic devices. Because neuroprosthetic devices are integrated into the neural circuitry of their human hosts, it is possible for an adversary to attack the device-host system by targeting either a neuroprosthetic device or the human being with whose structures and processes the device is so closely interconnected. A direct attack on the neuroprosthetic device itself might indeed typically target the device in its nature as an electronic computing device (e.g., through the use of computer viruses or worms or the use of a botnet to launch a denial of service attack). However, the possibility of neuroprosthetic devices that include biological material as key components<sup>39</sup> – or which even consist entirely

<sup>36</sup> See Ankarali et al., “A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security” (2014), p. 247.

<sup>37</sup> See Ankarali et al., “A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security” (2014), pp. 247–48.

<sup>38</sup> See Ankarali et al., “A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security” (2014), p. 247.

<sup>39</sup> For the possibility of neuroprosthetic devices that include biological components, see Merkel et al., “Central Neural Prostheses” (2007). A hybrid biological-electronic interface device (or “cultured probe”) that includes a network of cultured neurons on a planar substrate is discussed by

of biological material – opens the door to attacks that target a neuroprosthetic device (or component thereof) in its nature as a biological system rather than an electronic device. Such attacks might, for example, utilize genetically engineered biological (rather than computer) viruses, radiation, chemical toxins, or other vectors or agents that can damage living biological organisms or disrupt their functioning. The human host of a neuroprosthetic device could be subjected to a similar biological attack. Moreover, he or she is also vulnerable to a different kind of psychological attack that operates not primarily at the cellular level of electrochemical activity but at the higher level of cognitive activity such as perceptions, beliefs, and volitions. We can categorize such attacks in the following way:

- **Electronic attacks** are directed at a neuroprosthetic device in its nature as an electronic sensor, computing device, or actuator. Such attacks may utilize means that are often employed against traditional computers, such as computer viruses or worms, other kinds of malware, or denial of service attacks.<sup>40</sup> While such attacks target the neuroprosthetic device in its nature as an electronic device, the attack itself does not necessarily need to be delivered through electronic means; while a computer worm would typically be delivered through some electronic medium, an attack which (for example) uses a chemical agent or magnetic field to erase data stored on a neuroprosthetic device's internal magnetic storage unit would also be considered an electronic attack.
- **Biological attacks** target either a neuroprosthetic device or its human host in their nature as biological organisms. A biological attack could only be launched against a neuroprosthetic device that contains at least some biological material as components. Biological attacks can involve any agents or vectors that are capable of harming or disrupting the functioning of biological organisms, including bacteria, biological (rather than computer) viruses, chemical toxins, electromagnetic radiation, or excess heat, pressure, or other environmental conditions.
- **Psychological attacks** target the human host of a neuroprosthetic device at a level that affects, overpowers, disrupts, or requires the involvement of the host's cognitive processes at a higher level than that

---

Rutten et al. in "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe" (2007). Hybrid biological-electronic interface devices are also discussed by Stieglitz in "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems" (2007).

<sup>40</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), pp. 141-62, for a discussion of such threats.

of basic biochemical processes. Social engineering attacks<sup>41</sup> are a form of psychological attack. Other such attacks might target a host's memories, emotions, or beliefs by providing particular kinds of sense data (e.g., comprising written text, audiovisual materials, or social interactions) whose harmful effect is generated not by its immediate impact on the host's sensory organs at the biochemical level, but through the cognitive processes by which the host perceives and interprets the experience and incorporates it into his or her memory. At present, psychological attacks can only be launched against the human host of a neuroprosthetic device, however if a future neuroprosthetic device possessed a sufficiently sophisticated form of artificial intelligence, it could potentially be subject to psychological attacks as well.<sup>42</sup>

- **Hybrid attacks** utilize more than one attack modality at the same time. An example might be a computer virus that infects an implanted neuroprosthetic device, takes control of the device, and uses it to produce chemical agents that are released into the bloodstream of the device's human host in order to effect a biological attack on the host. Conversely, a genetically engineered virus or other biological agent could be introduced into a host's bloodstream, where it infects the biological component of an implanted neuroprosthetic device and introduces instructions in the form of genetic material (rather than executable computer code) that will cause the biological component of the neuroprosthetic device to influence, disrupt, control, or even reprogram the electronic component of the neuroprosthetic device in such a way that will constitute an electronic attack.<sup>43</sup>

The growing convergence of fields such as neuroscience, genetic engineering, bionanotechnology, and molecular computing<sup>44</sup> along with the increasing integration of the human organism into biocybernetic and neurocybernetic systems means that hybrid attacks against neuroprosthetic devices and their device-host systems are likely to become increasingly common. The most sophisticated kinds of attack agents may even be able to shift repeatedly

---

<sup>41</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), pp. 307-23.

<sup>42</sup> See Friedenber, *Artificial Psychology: The Quest for What It Means to Be Human* (2011), for an in-depth analysis of psychological effects to which future AI systems (and in particular, artificial general intelligences) might be subject.

<sup>43</sup> Some future neuroprosthetic devices with biological components might conceivably be designed to store program or data files in the form of genetic material; a virus or other biological agent that is able to rewrite the contents of that genetic material could, in effect, "reprogram" the device – potentially in a way that would in turn lead to an alteration in the contents of program or data files stored by the device in electronic format. For a discussion of the possibilities of using DNA as a mechanism for the storage of data, see Church et al., "Next-generation digital information storage in DNA" (2012).

<sup>44</sup> See Chapter Three of this text for a discussion of this convergence.



between electronic, biological, and psychological forms while preserving intact their specified payload and moving toward their ultimate target. The existence of such threats will require information security practitioners to collaborate closely with experts from fields such as neuroscience, biology, biomedical engineering, epidemiology, cybernetics, and other disciplines, in order to develop full-spectrum information security plans, mechanisms, and practices that can protect against electronic, biological, psychological, and hybrid attacks.

***Attacks on, through, or with a neuroprosthetic device***

We can also distinguish three different kinds of attacks that relate to neuroprosthetic devices by identifying the role that a neuroprosthetic device plays in the attack:

- **Attacks on a neuroprosthetic device** are targeted against a particular neuroprosthetic device or its device-host system. While they might involve an electronic vector such as a computer virus that requires the adversary who is launching the attack to possess significant knowledge of the targeted device, they might instead involve a purely physical attack (e.g., using radiation, electricity, chemical agents, or a physical weapon such as a hammer) that does not require the adversary to possess a neuroprosthetic device or, in some cases, even to know exactly how to access or control the targeted device.
- **Attacks through a neuroprosthetic device** occur when an adversary hijacks (either temporarily or permanently) or otherwise exercises operative control over a neuroprosthetic device of which he is not the human host in order to utilize it in executing an attack. For example, if an individual possesses a cochlear implant that can record and wirelessly transmit live audio of everything that the person is hearing, an adversary might illicitly access that device and its live audio feed not in order to conduct surveillance on the person in whom the device is implanted, but in order to eavesdrop on the conversations of two people who at the moment happen to be sitting in a train car near that person and who are the adversary's ultimate target.<sup>45</sup>
- **Attacks with a neuroprosthetic device** occur when an adversary is the human host of a neuroprosthetic device that he or she uses as a tool for planning or executing attacks. The potential use of neuroprosthetic devices by adversaries in this manner raises complex biomedical, legal, and ethical questions for information security practitioners, insofar as

---

<sup>45</sup> See Chapter Three of this text for further discussion of such possibilities.

certain kinds of countermeasures that might be utilized to prevent a cyberattack or mitigate an ongoing attack could potentially have a direct negative impact on the physical and psychological health of the adversary conducting the attack, if the computer that the adversary was using to manage the attack (and which is affected – and possibly disrupted or even disabled – by the countermeasures) is a neuroprosthetic device that is integrated into the neural circuitry of the adversary’s biological organism.<sup>46</sup>

Depending on its nature, it is possible for a single attack to be committed simultaneously on, through, and with neuroprosthetic devices.

### *Other notable types of attacks*

Researchers have identified other kinds of possible attacks that technically can be classified using one of the schemes above (e.g., as either “passive” or “active”), but which merit specific mention here either because they have the potential to cause particularly devastating effects or are unique to neuroprosthetic devices. Such attacks include:

- **Long-term neural modifications.** Denning et al. note that some attacks on neuroprosthetic devices might be intended by an adversary to generate some long-term changes in the cognitive processes of a device’s host.<sup>47</sup> In addition to affecting biological processes such as the functioning of internal organs, such changes could potentially impact the host’s memories, beliefs, personality, skills, habits, relationships, and other activities and phenomena rooted in cognitive processes and abilities.
- **Disruption of neural networks.** By gaining illicit access to a neuroprosthetic device and disrupting or controlling its functioning, an adversary could potentially harm the device’s host either by causing the death of existing cells or by disrupting neural networks through the growth of new cells or changes to existing cells.<sup>48</sup>
- **Induced addictions.** Some kinds of neuroprosthetic devices may be designed to function (or, if damaged or maliciously reprogrammed, be capable of functioning) in a way that could create an addiction within a device’s human host. Denning et al. note that some neuroprosthetic

---

<sup>46</sup> For a discussion of some of the legal and ethical issues that are involved, e.g., with the contemporary use of offensive countermeasures to mitigate botnets, see Leder et al., “Proactive Botnet Countermeasures: An Offensive Approach” (2009). The issue is also discussed further in Chapter Three of this text.

<sup>47</sup> See Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

<sup>48</sup> See Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

devices may reduce pain, change their host's mood, or activate pleasure and reward centers within the brain<sup>49</sup> in a way similar to found with opioid analgesic drugs. Such euphoric or other effects could potentially be produced either indirectly, by releasing chemicals or other agents into the host's bloodstream, or directly by electrically stimulating relevant portions of the host's brain.

We would suggest that an adversary who is able to take control of such a neuroprosthetic device could potentially induce an addiction on the part of its host (perhaps even gradually, with the host not fully realizing what was occurring) and then threaten the host with termination of the addictive effects (and the infliction of resulting withdrawal symptoms) unless the host performs or fails to perform some action, as instructed by the adversary. The manufacturers or operators of certain kinds of neuroprosthetic devices could potentially use a similar approach conceptualized not as an "attack" but as a "business strategy" designed to increase the painful switching costs that a device's host would experience if he or she were to discontinue use of the device or to require ongoing purchases or subscriptions in order to continue experiencing the addictive neuroprosthetic effects.<sup>50</sup>

- **Resource depletion attacks.** Resource depletion attacks are a kind of denial of service attack that aims to disable or disrupt an implanted device by exhausting one of its critical resources – typically the power supply contained within its internal battery.<sup>51</sup> Resource depletion attacks are of critical concern for implantable neuroprosthetic devices, because after its implantation a device's store of certain resources (such as electrical power or chemical agents to be injected into the host's bloodstream) may be quite limited and not easily replenishable. Resource depletion attacks can easily be launched against implantable devices if their security controls have not been appropriately designed and implemented: for example, if an implantable device carries out some specified action that consumes electrical power (such as transmitting an RF signal to the external system in response) every time it

---

<sup>49</sup> See Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

<sup>50</sup> For an analysis of how such possibilities have been explored within a fictional setting, see Maj, "Rational Technotopia vs. Corporational Dystopia in 'Deus Ex: Human Revolution' Gameworld" (2015).

<sup>51</sup> See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011), and Freudenthal, et al., "Practical techniques for limiting disclosure of RF-equipped medical devices" (2007).

detects that a wireless access request has been received from an external system, an adversary could potentially quickly exhaust the implant's battery and disable the implant simply by sending an unending series of wireless access requests to the device, even if all of the access requests were rejected by the implant.

Having considered fundamental information security concepts such as the CIA Triad, administrative, logical, and physical security controls, authentication and authorization, and the distinction between vulnerabilities, threats, and risks, in the next chapter we will explore in more detail many of the unique challenges that arise when attempting to apply these principles in the case of advanced neuroprosthetic devices.



## Chapter Three

# Critical Challenges in Information Security for Advanced Neuroprosthetics

### Information security considerations unique to advanced neuroprosthetics

Information security is a large and complex field. While there are fundamental information security principles whose relevance is universal, the ways in which these principles are applied and elaborated in particular circumstances is subject to specialized practices and bodies of knowledge. The techniques used to secure a large organization's archive of decades of printed personnel files are different than those used to secure a factory's robotic manufacturing systems or an individual consumer's smartphone.

As with all kinds of information systems that have been developed by humankind, advanced neuroprosthetic devices present a unique array of information security problems and possibilities that exist within a particular set of technological, legal, political, ethical, social, and cultural contexts.<sup>1</sup> In this chapter we highlight a number of issues that may not be relevant for many other kinds of information systems but which give rise to considerations that are critical for the information security of advanced neuroprosthetic devices. Many of the issues discussed below constitute recurring themes that will be revisited in different contexts throughout the rest of this book.

### Device user vs. device host

In the case of a smartphone, the person who possesses the device and carries it with himself or herself on a daily basis is typically also the primary user and operator of the device: the smartphone's possessor powers it on and off,

---

<sup>1</sup> For an overview of ethical issues with ICT implants – many of which are relevant for advanced neuroprosthetics – see Hildebrandt & Anrig, “Ethical Implications of ICT Implants” (2012). For ethical issues in information security more generally, see Brey, “Ethical Aspects of Information Security and Privacy” (2007).

uses it to browse the web, check email, make calls, and play games, and downloads, installs, and uninstalls apps at will. In some institutional settings, a smartphone that is owned by the organization may not be controlled entirely by the person who possesses it; the organization's IT staff might remotely control and monitor some aspects of the phone's behavior and might, for example, restrict its possessor's ability to install new apps. However, the person possessing the phone still has a significant ability to control the device's settings and operation and to use its functionality to achieve his or her personal ends.

With advanced neuroprosthetic devices (and implantable medical devices generally) the situation can be quite different: a device's host – i.e., the human being in whose body the neuroprosthetic device is implanted and in which it operates – may have no ability whatsoever to control the device or to utilize its functionality for particular ends chosen by that person. Moreover, he or she may not even realize that the device exists and has been integrated into his or her neural circuitry.

#### **SHARED OPERATION AND USE BY THE HOST AND AN EXTERNAL PARTY**

In the case of an artificial eye, for example, it might be the case that the device's human host has full operational control over the device: through an act of volition, the host transmits instructions that cause the eye to focus its gaze on particular objects, and by using a standard computer the host can wirelessly connect to the artificial eye's internal computer, log onto a web-based command console, and perform remote diagnostics and software maintenance on the device.

On the other hand, it might be the case that the device's human host is only able to control some limited aspects of the artificial eye's functionality (such as determining its focus or dilating its synthetic pupil) but has no ability to log into the device to manage diagnostic or maintenance tasks; a remote support team of specialized medical and biomedical engineering experts (e.g., working at the company that designed the device or the hospital that implanted it) may be the only party with such access – regularly monitoring the device's functioning, performing remote software upgrades and reconfiguration, and managing aspects such as the device's power consumption and synaptic stimulation strength. In such a scenario, the human being in whom the artificial eye was implanted would be the device's human *host*, but the host and the remote medical team would share a joint role as the device's *users* or *operators* who determine how and for what purposes it will be used and who control its functionality.

### SEPARATE OPERATOR AND HOST

It is also possible to envision circumstances in which a device's human host would play no role at all in controlling the device, determining the purposes for which it will (or will not) be employed, or managing its functionality. In such cases, another human being or organization may serve as the sole user and operator of the device, or, if the device possesses sufficiently sophisticated artificial intelligence, the device could even be said to be its own user and operator.

For example, a human host suffering from a particular illness may have been implanted with an endocrine neuroprosthetic device that can stimulate the host's thyroid gland and cause it to secrete hormones that affect the body's basal metabolic rate; however, the host has no means or access by which to control (or even directly influence) the functioning of the device, as it can only be controlled through a remote system that wirelessly transmits instructions to the device and is managed by an expert medical team. The medical team constitutes the device's sole user and operator, as team members decide when, whether, and to what extent the host's basal metabolic rate should be raised or lowered, and the medical personnel determine the objective (e.g., to facilitate weight loss or weight gain) that they are seeking to achieve through their management of the device.<sup>2</sup>

### UNWITTING HOSTS

Especially in the case of noninvasive neuroprosthetic devices that can connect with the neural circuitry of a human being simply by touching the person's body (or even without touching it, through the use of wireless transmission and sensation), it may be possible that the human being with whose neurons the device is interacting may not even realize that the device exists or is in use. Even in the case of neuroprosthetic devices that can only function within the body of their human host, a device's host may potentially not realize that a neuroprosthetic device is located and operating within his or her body – e.g., if unbeknownst to the subject the device was implanted during the course of some other surgical procedure to which the host had consented, or if the device comprised components (such as a swarm of nanorobots) that could be unwittingly ingested by consuming a beverage.<sup>3</sup>

---

<sup>2</sup> Another possible cybernetic model is for a system to include an implanted component that gathers from its host's brain selected real-time data that is then transmitted to an external system and used as input for a real-time computational model and simulation of the brain that allows the device's operators to determine what signals the implanted component should transmit to neurons in order to generate desired effects; the external system then transmits those instructions to the implanted component, which then stimulates neurons in accordance with those instructions. See Lee et al., "Towards Real-Time Communication between in Vivo Neurophysiological Data Sources and Simulator-Based Brain Biomimetic Models" (2014).

<sup>3</sup> For the possibility that human hosts might unwittingly have been implanted with RFID devices,



**PHYSICAL AND PSYCHOLOGICAL DAMAGE CAUSED TO USER OR HOST**

In numerous contexts throughout this text, we cite the possibility that a neuroprosthetic device that is poorly designed and operated, suffers a malfunction, or is compromised by a cyberattack could potentially subject its human host to significant physical or psychological harm – e.g., by impairing the functioning of the host’s internal organs or providing a stream of sensory data that causes severe pain. While such harm to a device’s host may be the more common hazard, with some kinds of neuroprosthetic devices it possible that such incidents might cause physical or psychological harm to the device’s human *operator* rather than its *host*.

For example, imagine that a human host has – without his or her knowledge – been implanted with an advanced neuroprosthetic device located in the brain that detects sense data arriving from the optic and cochlear nerves and wirelessly transmits it to another human being – the device’s operator – who through the use of a virtual reality headset and earphones is essentially able to see and hear all that the neuroprosthetic device’s human host sees and hears. An adversary could potentially gain unauthorized access to the neuroprosthetic device’s internal computer, reprogram it, disable its safety features, and alter its output so that rather than transmitting to the device’s remote human operator a stream of the actual visual and auditory sense data received by the device’s host it instead transmitted signals which, in the operator’s VR headset and earphones, produce an emission of blinding light and deafening noise that are powerful enough to both damage the operator’s sensory organs, cause confusion and disorientation, and inflict major psychological distress. Note that if the operator (and, in this case, end user) of the neuroprosthetic device were receiving the transmitted sense data not through a conventional VR headset and set of earphones but through a neuroprosthetic implant within his or her own brain, then an arrangement would exist in which that individual was simultaneously serving as the host of one neuroprosthetic device and the operator of (potentially) two devices, and the damage would result from the person’s roles both as host of his or her own implanted device and operator of the remotely controlled one.

**Critical, noncritical, or no health impacts for a device’s host and user**

A conventional desktop computer is unlikely to have a direct critical impact (either positive or negative) on the health of its human user. While it is

---

see Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012).

possible to imagine a critical health impact (e.g., if the computer electrocuted a user who had removed the outer casing and was attempting to repair the device or if the user dropped the computer and injured himself or herself while attempting to carry it to a new location), such impacts involve highly unusual circumstances and do not result directly from the success or failure of the computer to perform its intended regular functions. It is perhaps more likely for a computer to have an impact on its user's health that is critical but highly indirect – e.g., by allowing its user to contact emergency medical personnel and summon assistance with some urgent health emergency or to research symptoms that the user was experiencing and diagnose a major illness.

Because of their intimate integration into the body and biological processes of their human host, however, neuroprosthetic devices have the potential to directly generate critical health impacts for human beings that other kinds of information systems are unlikely or unable to produce.<sup>4</sup> For example, the failure of a neuroprosthetic device that is responsible for regulating its host's respiratory or circulatory activity could result directly in the host's death within a matter of minutes or even seconds; conversely, the proper functioning of the device may extend its host's lifespan by many years. Such devices clearly possess a critical health impact.

Other kinds of technology, such as a neuroprosthetic robotic leg, may typically have a significant but indirect and noncritical impact on the health of its user. When functioning properly, the leg allows its user to stand and balance without falling and to walk, run, and exercise – all of which can contribute significantly (if not critically) to the user's health. On the other hand, if the device experiences a malfunction that gives the user mild electrical shocks or requires the user to drag the immobile leg, such occurrences would constitute undeniably negative but generally noncritical health effects. Such device malfunctions call for prompt attention and maintenance but do not require an immediate response in order to save the life of the device's host.

Even with devices that generally demonstrate noncritical health impacts, it may be possible for them to yield a critical health impact in particular circumstances. For example, if an artificial eye were to fail while its host were driving an automobile or flying a helicopter, this could potentially have fatal consequences not only for the host but also for many other completely unrelated individuals. A similarly critical negative health impact could result if an adversary gained unauthorized access to the eye's internal computer and manipulated the device's sensory output to make its host believe, for example,

---

<sup>4</sup> For some of the health impacts that can be generated, for example, by IMDs (whether neuroprosthetic devices or other kinds of IMDs), see Ankarali et al., "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security" (2014).

that he or she was picking up a wooden stick from the lawn when in fact it was a poisonous snake.<sup>5</sup>

No matter how safe, limited, and benign its functionality might be, it is unlikely that any neuroprosthetic device could ever possess *no* health impact, insofar as it is by definition interacting with the neural circuitry of its human host. While some advanced devices might theoretically be able, for example, to remotely detect and interpret a human being's cognitive activity simply by relying on the passive capture of radiation or other phenomena naturally emitted by the person's brain – and thus allow the person to control some remote robotic system through thought alone – such a device would not be considered a “neuroprosthetic device” according to the definition of this text, since it is not truly *integrated into* the neural circuitry of the person's brain or body in any substantive sense.

Note that when a neuroprosthetic device possesses (or has the potential to demonstrate) a critical health impact, ensuring information security for the device and its host and user becomes even more important than usual. The greatest possible attention to information security must be shown by such a device's designer, manufacturer, operator, and host; such a device is likely to need extremely robust and stringent security controls that may not be necessary for devices with a lesser potential health impact. This obligation to ensure the highest possible degree of information security for neuroprosthetic devices with a (potentially) critical health impact will inform our discussions of many specific security practices and mechanisms throughout this text.

### **Lack of direct physical access to implanted systems**

Because of the risks and difficulties involved with surgical procedures, after a neuroprosthetic device has been implanted in its human host, information security personnel working to protect that device and its host may never again enjoy the opportunity to physically inspect, manipulate, or otherwise access the device; from that point forward, the only means of interacting with the device may be through wireless communication<sup>6</sup> (assuming that the device possesses such capabilities) or through action of the device's host (e.g.,

---

<sup>5</sup> For the possibility that sensory neuroprosthetics might be used to supply false data or information to their hosts or users, see McGee, “Bioelectronics and Implanted Devices” (2008), p. 221.

<sup>6</sup> For an overview of information security issues relating to the wireless communication of IMDs such as body sensor networks (BSNs) – many of which are relevant for advanced neuroprosthetics – see Ameen et al., “Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications” (2010).

if the host has the ability to communicate with, influence, or control the device through acts of volition or other internal cognitive or biological processes). On the one hand, such limitations in physical access may create challenges for information security personnel: for example, it may be necessary to build into a device at the time of its creation and implantation security controls that will be powerful and adaptable enough to counteract threats that may not yet even exist and will be developed only years or decades after the device's implantation. Moreover, some physical security controls that can be applied to conventional computers (such as the use of hardwired rather than wireless communication between devices) may be impossible to apply to an implanted device that exists beyond one's grasp and direct physical control. On the other hand, the fact that a neuroprosthetic device has been implanted in a human host might also bring some security benefits (such as physical concealment of the device's existence<sup>7</sup>) that are more difficult to implement in other kinds of information systems such as desktop computers.

### 100% availability required

From the perspective of information security, the information contained within particular information systems can be said to demonstrate “availability” if the “systems work promptly and service is not denied to authorized users;”<sup>8</sup> other information security experts have defined availability as “Ensuring timely and reliable access to and use of information”<sup>9</sup> or the “Usability of information for a purpose.”<sup>10</sup> These are the meanings of availability that are intended, for example, when the word is used as part of the CIA Triad of information security objectives.

Other branches of computer science and information technology, however, use the word “availability” with an equally specific but somewhat different meaning: in that alternative sense, an information system's availability is a quantitative measure of how likely it is that the system will be operational (i.e., not out of service due to some hardware or software fault) at a given point in time. One can quantify a computer's **reliability** as the **mean time to failure** (MTTF), or the average length of time that a system will remain in continuous operation before experiencing its next failure,<sup>11</sup> while the **mean**

<sup>7</sup> Regarding the use of physical concealment in protection information systems, see *NIST SP 800-53*, Rev. 4 (2013), p. F-205-F-206.

<sup>8</sup> *NIST SP 800-33* (2001), p. 2.

<sup>9</sup> 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37*, Rev. 1 (2010), p. B-2.

<sup>10</sup> See Parker, “Toward a New Framework for Information Security” 2002, p. 124.

<sup>11</sup> See Grottke et al., “Ten fallacies of availability and reliability analysis” (2008), as cited in Glad-den, “A Fractal Measure for Comparing the Work Effort of Human and Artificial Agents Performing Management Functions” (2014), from which this section on availability is adapted.

**time to repair** (MTTR) is the average length of time needed to detect and repair a failure after it has occurred and thereby return the system to operation. A computer's steady-state **availability**  $A$  can be defined as the likelihood that the system is operating at a particular moment; it is related to the system's MTTF and MTTR by the equation:<sup>12</sup>

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

A typical requirement for general-purpose commercial computer systems is that they demonstrate 99.99% availability over the course of a year.<sup>13</sup> However, in the case of some neuroprosthetic devices that level of availability could be wholly unacceptable, insofar as it would represent an average of roughly 53 minutes of downtime over the course of a year. With some kinds of advanced neuroprosthetic devices that regulate critical circulatory or respiratory functions within their host's body, the impact of a device ceasing to operate for a period of 53 consecutive minutes could prove fatal to its human host. On the other hand, for other kinds of devices a period of 53 consecutive minutes in which the device was nonfunctional might not be particularly harmful – especially if the outage took place as part of a scheduled repair process and a medical support team was ready to monitor and treat the device's host during that period, or if the host possessed a reliable backup system that he or she could easily activate during the one hour a year when the primary device typically became nonfunctional.

For some kinds of neuroprosthetic devices, a single long outage once per year might be less harmful than many frequent outages of shorter duration. For example, a system that freezes up and becomes nonfunctional for one millisecond out of every 10 seconds would also demonstrate roughly 99.99% availability. If such a neuroprosthetic device serves as the controller of a complex device network in which it receives data from and coordinates the actions of a number of other implanted devices regulating its host's core biological functions, such frequent outages could potentially impair the work of the entire system – especially if the system needs a couple of seconds to confirm the system's integrity and regain full operational capacity after each millisecond outage.

---

<sup>12</sup> See Grottke et al., “Ten fallacies of availability and reliability analysis” (2008).

<sup>13</sup> See Gunther, “Time—the zeroth performance metric” (2005).

The question of how much time is needed to *fully recover* complete operational capacity by a system whose outage has already ended and which is already nominally functional raises another question relating to availability. In the sense just described here, availability has traditionally been understood in a binary manner: a system is either “up” or “down,” with no possible states in between.

While the binary definition of availability is conceptually elegant and results in an equation that is easy to apply, the binary definition completely fails to capture many of the difficult realities with which IT professionals must often grapple. For example, if a hardware failure, software configuration error, or denial of service attack dramatically impacts an organization’s information system and reduces the system’s performance to only 0.5% of its normal processing speed and capacity, the lived experience of many people in the organization may be that the system is experiencing a catastrophic outage and is wholly nonfunctional. However, according to the technical definition of availability just given, one would say that the system has not “failed,” because the system has not failed *completely*; although the system’s performance has been dramatically degraded, the system is still operational and functional – simply at a reduced level of speed and capacity. In order to address such limitations with the binary definition of availability, Rossebeø et al. argue that a more sophisticated measure for availability is needed that takes into account qualitative aspects of a system’s performance and which recognizes a range of intermediate qualitative states between simply “up” and “down.”<sup>14</sup> This is especially true for many kinds of advanced neuroprosthetic devices.

For example, imagine that a high-resolution artificial eye provides its host with output sense data corresponding to a field of vision consisting of five million pixels; that is arguably roughly comparable to the resolution offered by a natural human eye.<sup>15</sup> When operating at such a level, one could say that the system is fully operational and that both the information system (constituted by the artificial eye) and the system’s information (constituted by raw sense data from the external environment that has been processed by the device and outputted to its human host) are available. However, during moments of especially high demand on the device’s internal processor (e.g., when it is performing a major diagnostic operation or undergoing a software

---

<sup>14</sup> See Rossebeø et al., “A conceptual model for service availability” (2006).

<sup>15</sup> The question of the human eye’s “resolution” is quite complicated. While an eye contains many more than one million sensors (i.e., individual rods and cones), there are only about one million output neurons (in the form of ganglion cells) that transmit data from the eye to the brain, and roughly half of the data comes from the tiny fovea, or focal point at the center of the field of vision in which the eye provides sharp central vision. See Linsenmeier, “Retinal Bioengineering” (2005), for a discussion of some such issues.

upgrade) the field of vision provided by the device's output data degrade to perhaps, say, only 5,000 total pixels. Although this would represent a dramatic 99.9% reduction in performance (as measured by resolution), it would still be sufficient to allow its host to carry out such tasks as navigating around a room, recognizing faces, or reading text on a computer screen.<sup>16</sup> If one were restricted to a binary definition of availability, one would need to say that the information system and its information were both "available," because the system was indeed functioning and making information available, if to a limited degree.

Imagine further that a major sensor component within the artificial eye fails and the device switches instantaneously to a rudimentary backup sensory of quite limited capacity: as a result, the output data produced by the device represents a visual field of only 64 total pixels. Such limited visual data would likely be insufficient to give the device's host the ability to perform even basic tasks such as navigating visually around a room or recognizing a particular face. In this situation, a binary measure of availability would tell us that the information system and information are still available: the device, after all, is functioning and providing its human host a constant stream of data that represents (in a very limited fashion) the raw sense data received from the external environment. However, from the perspective of information security it would be difficult to say without qualification that the information system and its information were "available" in the sense envisioned by the CIA Triad. If an adversary had launched a cyberattack and gained unauthorized access to the artificial eye in an effort to steal visual information that reveals where the device's host is and what he or she is doing, the adversary would likely not feel satisfied with gaining access to a display of 64 pixels that contains no practically interpretable, *useful* information about the host's external environment or the host's activities.

When considering "availability" in its sense of the functionality or operability of an information system, one must thus carefully consider whether the measure should be defined in a binary manner in which "availability" signifies any non-zero level of functionality; whether the measure should be defined in a binary manner in which "availability" signifies a level of functionality greater than some particular specified non-zero threshold; or whether a non-binary, multivalent understanding of availability is more appropriate.

For certain kinds of neuroprosthetic devices with critical health impacts, simply setting and meeting a target like 99.99% availability or even 99.999%

---

<sup>16</sup> See Weiland et al., "Retinal Prosthesis" (2005), and Viola & Patrinos, "A Neuroprosthesis for Restoring Sight" (2007).

availability (the so-called “five nines” level of availability, equivalent to roughly five minutes of downtime per year) may not be sufficient, as such periods of downtime could be harmful or even fatal to the devices’ human host. For some kinds of devices, the only target that is acceptable from a legal and ethical perspective may be that of 100% availability – even if it is known in advance that this may be unattainable, due to circumstances beyond the control of a device’s designer, manufacturer, operator, or host. The existence of critical health impacts and the need for 100% availability can be understood in relation to the concept of a zero-day vulnerability in information security, in which software or hardware developers must work as quickly as possible to develop a patch or fix for an uncorrected flaw.

### The need for rigorous security vs. the need for instant emergency access

The fact that advanced neuroprosthetic devices are integrated into the neural circuitry of their human host creates a unique information security challenge – and potentially a dilemma – for the developers of such technologies.

#### THE NEED TO PROTECT A DEVICE FROM UNAUTHORIZED PARTIES

On the one hand, a neuroprosthetic device ought to be better secured against computer viruses and unauthorized access than, say, its host’s laptop computer or smartphone. After all, if a person’s smartphone is compromised, it could potentially result in inconvenience, financial loss, identity theft, the disclosure of sensitive and embarrassing information, and potentially even legal liability for that person – but it is unlikely to have a direct critical impact on the person’s physical health. If a person’s neuroprosthetic device is compromised, though, this might not only allow an adversary to steal sensitive medical data and information about the person’s cognitive activity (potentially even including the contents of sensory experiences, memories, volitions, fears, or dreams); it might also – through the device’s impact on the person’s natural neural networks – have the effect of rendering damaged, untrustworthy, or inaccessible the information stored within the host’s natural biological systems, including the brain’s memory-storage mechanisms.<sup>17</sup> The potential impact of the intentional manipulation or accidental corruption of a neuroprosthetic device could be potentially catastrophic for the physical and psychological health of its human host; this suggests that access to such a device should be limited to the smallest possible number of human agents

---

<sup>17</sup> For the possibility that an adversary might use a compromised neuroprosthetic device in order to alter, disrupt, or manipulate the memories of its host, see Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).



who are critical to its successful functioning, such as the device's human host and – if a different person – its primary human operator.

#### **THE NEED TO GRANT EMERGENCY DEVICE ACCESS TO OUTSIDE PARTIES**

On the other hand, though, there are reasons why restricting access to a neuroprosthetic device too severely might also result in significant harm to the device's host. For example, imagine that the human host of a neuroprosthetic device has been involved in a serious accident or is unexpectedly experiencing an acute and life-threatening medical incident. In this case, emergency medical personnel on the scene may need to gain immediate access to the neuroprosthetic device and exercise unfettered control over its functionality in order to save the life of its host.<sup>18</sup> The same mechanisms that make it difficult for a cybercriminal to break into the neuroprosthetic device – such as proprietary security software, file encryption, and a lack of physically accessible I/O ports – would also make it difficult or impossible for emergency medical personnel to break into the device. In principle, government regulators could require (or the manufacturers of neuroprosthetic devices could voluntarily institute) mechanisms that allow such devices to be accessed by individuals presenting certain credentials that identify them as certified emergency medical personnel who are trained in the use of such technologies,<sup>19</sup> or neuroprosthetic devices could be designed to temporarily disable some of their security controls if they detect that their host is experiencing a medical emergency.<sup>20</sup> However, such mechanisms themselves create security vulnerabilities that could potentially be exploited by an adversary who is highly motivated to gain access to the information contained in a neuroprosthetic device or its human host.

#### **PROPOSED METHODS FOR BALANCING THESE COMPETING DEMANDS**

Ideally, a neuroprosthetic device (and especially one with a critical health impact for its host) would be utterly impervious to all attacks and impenetrable to any adversaries attempting to gain unauthorized access – but would

---

<sup>18</sup> See Clark & Fu, “Recent Results in Computer Security for Medical Devices” (2012); Rotter & Gasson, “Implantable Medical Devices: Privacy and Security Concerns” (2012); and Halperin et al., “Security and privacy for implantable medical devices” (2008) – all of whom who make this point regarding IMDs. Halperin et al., especially, consider this question in detail.

<sup>19</sup> For a discussion of such certificate schemes and related topics, see, for example, Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012), and Freudenthal et al., “Practical techniques for limiting disclosure of RF-equipped medical devices” (2007).

<sup>20</sup> Regarding the ability of IMDs to detect a medical emergency that is being experienced by their human host, see Denning et al., “Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010), pp. 921–22.

instantaneously grant full access and place itself at the disposal of any trained and well-intentioned individual who, in time of need, was attempting to use the device to save its human host's life. In reality, it is difficult to design a device that simultaneously fulfills both of these visions, and trade-offs often need to be made. The priorities that a particular host adopts for his or her neuroprosthetic device's information security plan may partly depend on what the host considers to be more likely: that a corporate espionage agent or cybercriminal will someday attempt to break into his or her neuroprosthetic device in order to steal the person's memories or arrange the person's death, or that an emergency medical technician will someday need to break into the device and override its programmed functioning in order to deliver life-saving medical treatment or prevent the host from suffering some grave neurological damage.

Hansen and Hansen note that the controls and countermeasures designed to protect implantable medical devices from unauthorized access while simultaneously ensuring that authorized parties (such as emergency medical personnel) receive access typically take one of three forms, as either **detective**, **protective**, or **corrective** countermeasures. For example, a security control that alerts a device's human host to a series of unsuccessful logon attempts would be detective, one that blocks wireless transmissions from reaching an implanted device would be protective, and one that allows compromised data within the device's internal memory to be replaced by backup data from an external system would be corrective.<sup>21</sup> Below we consider a number of specific controls and countermeasures that have been proposed to address the challenge of providing both rigorous protection for implanted devices and robust emergency access for authorized personnel. While some of these approaches may not be relevant for all kinds of neuroprosthetic devices (especially devices that operate outside of their host's body), many of the approaches are relevant for implantable neuroprosthetic devices, and they offer an excellent starting point for considering issues of emergency access for neuroprosthetic devices more broadly.

#### **CERTIFICATE SCHEMES AND PREDEPLOYED KEYS MANAGED BY DEVICE MANUFACTURERS OR OPERATORS**

One approach to addressing this challenge involves the creation of a centrally managed worldwide certification scheme that would be administered either by a device's manufacturer or operator. At the time of its manufacture or implantation, a pre-configured backdoor key can be installed in the operating system of an IMD; the backdoor key can be maintained by the device's

---

<sup>21</sup> See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

manufacturer or operator in a cloud-based system that can be accessed globally through the Internet by medical personnel who are treating the device's host during the course of a medical emergency.<sup>22</sup>

However, this model demonstrates significant limitations and disadvantages. Hei and Du note that this “certificate” approach would fail in cases where the medical emergency (and treatment) were occurring in a location in which the personnel providing medical treatment did not have immediate Internet access (e.g., if an accident occurred in a remote wilderness area where wireless Internet access was absent or unreliable); moreover, they note that maintaining such a system of backdoor keys that are always accessible online would be complex and costly.<sup>23</sup>

#### **AN EXTERNAL HARDWARE TOKEN WHOSE POSSESSION GRANTS ACCESS TO THE IMPLANTED DEVICE**

Bergamasco et al. explore the use of hardware tokens such as a small USB token that can be inserted into a standard USB port as means of authenticating users of medical devices and information systems.<sup>24</sup> External hardware tokens that utilize wireless technologies – such as an RFID tag worn or carried by the host of a neuroprosthetic device – could potentially be used by the implanted device to wirelessly authenticate its user; even technologies such as a USB token that require physical insertion of the token into the implanted device could conceivably be used for authentication if the implanted device possesses a port, slot, or other component that is accessible from the exterior of its host's body. Denning et al. describe a similar approach of “proximity bootstrapping” in which emergency medical personnel who may come into contact with patients possessing implantable medical devices could be given a portable unit that can communicate with an IMD through sound waves or “physiological keying” when brought into contact with the device's host to request access to the IMD.<sup>25</sup>

---

<sup>22</sup> For a discussion of such matters, see, for example, Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012), and Freudenthal et al., “Practical techniques for limiting disclosure of RF-equipped medical devices” (2007).

<sup>23</sup> See Hei & Du, “Biometric-based two-level secure access control for implantable medical devices during emergencies” (2011).

<sup>24</sup> See Bergamasco et al., “Medical data protection with a new generation of hardware authentication tokens” (2001). They do not specifically consider the case of implantable medical devices but instead consider access to medical devices and information systems more generally.

<sup>25</sup> See Denning et al., “Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010), p. 922.

Hei and Du note that such an external hardware token can be lost (thus denying emergency access to an authorized party who has misplaced his or her token) or stolen (thus potentially granting access to an unauthorized party who has stolen or found the device).<sup>26</sup> We would also note that unless there is international regulation or extensive industry-wide (and even inter-industry) collaboration between the manufacturers of diverse kinds of implantable devices to agree on a single shared scheme for such tokens, the need for emergency personnel around the world to carry a bewildering array of tokens for different manufacturers' devices (and perhaps to test them all on every newly encountered patient in order to check whether any implanted devices might exist) could become unwieldy. On the other hand, if all device manufacturers were to utilize a single shared token system, this would give potential adversaries a lone attractive target on which to concentrate all of their efforts to compromise such devices.

#### **A CRYPTOGRAPHIC KEY STORED ON THE HOST'S PERSON**

One design for a security control is for wireless access to an implanted device to be secured using a cryptographic key (e.g., consisting of a string of characters) that must be possessed by any other implant or external device that wishes to access the implant. The cryptographic key – along with instructions to emergency medical personnel describing the nature of a host's implanted device and how medical personnel should access and configure the device during particular kinds of medical situations – could then be displayed on a standard medical bracelet worn by the device's host, similar to the sort that is already commonly used by individuals to alert emergency medical personnel to the fact that, for example, they suffer from diabetes or asthma or possess a pacemaker. However, such bracelets are not extremely secure: they can potentially be lost or stolen, may actually alert adversaries to the presence of an implantable device that they otherwise would not have known about, and (depending on their design) could potentially allow an adversary to photograph or otherwise obtain the information contained on the bracelet without even directly contacting it.<sup>27</sup> A card displaying the cryptographic key or password for an implanted device that is carried in the wallet of the device's human host<sup>28</sup> is less visible to potential adversaries while still likely to be found by emergency medical personnel treating the host.

---

<sup>26</sup> See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011).

<sup>27</sup> See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010), and Schechter, "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices" (2010).

<sup>28</sup> See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010).

Denning et al. and Schechter propose an access control method for implantable medical devices that utilizes ultraviolet-ink tattoos.<sup>29</sup> In this approach, an IMD is secured using a cryptographic key consisting of a string of characters. These characters can then be tattooed on the body of the device's host using a special ink that only becomes visible under ultraviolet light. Schechter notes that unlike a wearable accessory such as a bracelet that is used to store the cryptographic key, a tattoo cannot be lost or misplaced by a device's host; moreover, the existence of the tattoo is not readily apparent to potential adversaries, and if necessary the device's host could even prevent a suspected adversary from illuminating and reading the tattoo simply by applying sunscreen that sufficiently blocks ultraviolet light. In comparison to the use of a bracelet, one disadvantage of this approach is the fact that emergency medical personnel would have no immediate indication that the tattoo exists; they would only know to search for a tattoo if they had some particular reason for suspecting that the human subject whom they were treating might possess an implantable device secured by such a cryptographic key. Moreover, emergency medical personnel might not always have the correct sort of UV light available. On the other hand, if the use of UV-ink tattoos for such purposes someday became widespread, then it could conceivably become a standard practice for medical personnel to carry such UV lights and check all patients for the presence of such tattoos. An alternative would be a traditional tattoo that is visible to the naked eye,<sup>30</sup> which would be more likely to be noticed by emergency personnel but would also be more likely to alert an adversary to the existence of an implanted device and allow him or her to obtain the cryptographic key from the tattoo (e.g., since depending on its location on the host's body it could potentially be photographed from a distance).

Denning et al. note that the same sort of severe accident or injury that might require a device's host to receive emergency medical treatment might also damage or destroy the information contained in a tattoo or a medical bracelet worn on the host's person, thus creating a significant disadvantage for such approaches.<sup>31</sup>

---

<sup>29</sup> See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), and Schechter, "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices" (2010).

<sup>30</sup> See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

<sup>31</sup> See Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), p. 920.

### ACCESS CONTROL BASED ON ULTRASONIC PROXIMITY VERIFICATION

Rasmussen et al. propose a model of access control for implantable medical devices in emergency situations that relies on ultrasound technology to verify the physical proximity of an external system attempting to gain access to the IMD. Under normal circumstances, the IMD would require an external system to possess a shared cryptographic key in order to grant the external system access to the IMD; however if the IMD detects that its host is undergoing a medical emergency, it then shifts into an “emergency mode” in which any external system is allowed to access the IMD, as long as it is within a certain predefined distance – with the distance determined by measuring the time required for ultrasound communications to travel between the IMD and external system.<sup>32</sup>

Hei and Du note that while relying on such ultrasound proximity detection as a primary security control would be inappropriate in normal everyday circumstances (as the control would only function successfully if it could be assumed that the device’s host would typically recognize an approaching adversary and prevent him or her from getting too close to the host), it could be appropriate for use in emergency circumstances; they also note that it could be difficult to integrate a sufficiently powerful and effective ultrasound receiver into some kinds of implantable devices.<sup>33</sup>

### PHYSICAL RADIO FREQUENCY SHIELDING OF AN IMPLANTED DEVICE

Hansen and Hansen suggest that a simple means of securing IMDs against wireless RF attacks would be for a device’s host to wear a shielded undershirt or shielded bandages applied to the skin that block or disrupt wireless communications. They note that such electromagnetic shielding would be relatively lightweight (thus not greatly inconveniencing the device’s host) and could easily be removed by emergency medical personnel who need to treat the host during a critical health situation.<sup>34</sup>

Such an approach is not without disadvantages when applied to advanced neuroprosthetic devices. For many human hosts, being required to wear a special shielded undershirt or bandages wherever they go (e.g., while at the beach or taking a shower) may be an undesirable inconvenience in their daily life, and some hosts might choose to temporarily remove the shielding during such situations, leaving them vulnerable to attack. Moreover, those hosts

---

<sup>32</sup> See Rasmussen et al., “Proximity-based access control for implantable medical devices” (2009). Regarding the possibility of IMDs being able to detect a medical emergency that is being experienced by their human host, see Denning et al., “Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010), pp. 921–22.

<sup>33</sup> See Hei & Du, “Biometric-based two-level secure access control for implantable medical devices during emergencies” (2011).

<sup>34</sup> See Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010).

whose neuroprosthetic devices are implanted in their brain would need to wear a shielded hat, wig, bandage, or other appliance on their heads at all times, which can be more awkward and inconvenient than wearing a shielded undershirt and may also serve to draw adversaries' attention to the fact that the person possesses a cranial neuroprosthetic device.<sup>35</sup> Finally, such shielding would potentially block not only wireless RF attacks created by adversaries but *all* wireless RF communications; this would be impractical and even dangerous to the host's health and well-being if the implanted device requires periodic instructions communicated wirelessly from an external system in order to operate correctly (or if an external system needs to receive periodic communications from the implanted device – e.g., containing real-time medical data from the host – in order to correctly configure and apply medical treatments and ensure the host's safety and health). Indeed, in such cases, it would be imperative for a device's host to ensure that an adversary did *not* surreptitiously alter the host's clothing or provide the host with clothing that includes shielding that would disrupt the proper functioning of the host's neuroprosthetic devices.

#### **SUBCUTANEOUS BUTTONS THAT GRANT ACCESS TO A DEVICE**

Hansen and Hansen also suggest the possibility of a subcutaneous button that is implanted beneath the surface of the host's skin and which can be activated by pressing the host's body at a particular location. When the button is pressed, the IMD temporarily enters a special programming mode that disables some of its security controls and allows the device to be remotely accessed and reprogrammed (e.g., through wireless transmissions) for a specified period of time.<sup>36</sup> Hansen and Hansen note that such a button might be prone to being pressed accidentally, thus its location and nature would need to be carefully chosen in order to minimize such possibilities.

We would argue that while perhaps not appropriate as a sole security control, such a device might be more effectively used in conjunction with other security controls. For example, if one needed to both press the button *and* possess a particular hardware token or remove shielding from the body in

---

<sup>35</sup> The "tin foil hat" found within popular culture as a stereotypical tool used by paranoid individuals to protect themselves from telepathic attacks and mind control might thus – while not the most effective approach to neural defense – be an idea not entirely lacking in substance. For an analysis of the RF-shielding properties of such devices, see Rahimi et al., "On the effectiveness of aluminium foil helmets: An empirical study" (2005). For a discussion of "psychotronics" in popular culture (as well as of supposed efforts on the part of military agencies to develop technologies that could potentially be used for remote mind control), see Weinberg, "Mind Control" (2007).

<sup>36</sup> See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

order to wirelessly access the implanted device, this would create greater security. Even including two different subcutaneous buttons in different parts of the body that need to be pressed simultaneously or within a certain window of time would increase security and reduce the likelihood of the device's wireless access controls being inadvertently disabled.

Another design question to be considered is whether the existence and nature of a subcutaneous button should be visible to the naked eye, visible only with the aid of particular equipment (such as an ultraviolet lamp), or wholly undetectable to outside parties. Making a button less easily detectable would decrease the changes that an adversary would discover its existence, while perhaps also making it more difficult for emergency medical personnel to notice that the host possesses an implanted neuroprosthetic device and successfully access it.

#### **AN EXTERNAL UNIT MAINTAINING THE SECURED STATE OF AN IMPLANTED DEVICE**

Denning et al. propose a model in which the host of an implanted medical device carries a secondary, external device (which they call a “Cloaker”) that controls the access that other external systems can gain to the implanted device. While they propose and consider several different variations on that theme, all of the cloaking approaches of this type share in common the fact that when the cloaking device is present, the implanted device can only be accessed by certain authorized parties; when the cloaking device is absent (or nonfunctional), the implanted device “fails open” into a state in which the implant responds to all access requests received from external systems. In the case of a medical emergency, medical personnel could access the implanted device simply by removing the cloaking device from the primary device's host.<sup>37</sup>

The IMD could potentially determine whether or not the external cloaking device is present by sending an “Are you there?” query to the cloaking device every time that some external system attempts to access the IMD, however Denning et al. note that this could expose the IMD to a denial of service attack in the form of a resource depletion attack that attempts to exhaust the IMD's battery simply by sending an unceasing series of access requests. Denning et al. thus suggest an alternative approach in which the IMD sends an “Are you there?” query to the cloaking device at periodic, nondeterministic intervals set by the device's designer; the designer could choose intervals that are brief enough to ensure that the IMD will fail open quickly enough in the case of a medical emergency but not so brief that the IMD's battery will be exhausted through frequent queries. Denning et al. note that one challenge for this model is to deal effectively with the possibility that an adversary could jam

---

<sup>37</sup> See Denning et al., “Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security” (2008).



the wireless communications between the IMD and cloaking device, thereby inducing the IMD to fail open into a nonsecured state in which the adversary can gain access to the implant. Another disadvantage is the fact that while the IMD's periodic "Are you there?" queries to the cloaking device may not consume large amounts of power, they do place some drain on the unit's power supply, which – as for many implantable devices – may be quite limited and difficult to replenish.

#### **AN EXTERNAL GATEWAY THAT JAMS COMMUNICATION WITH THE IMPLANTED DEVICE**

Zheng et al. propose a model in which the host of an implanted device also wears or carries an external "gateway" device that controls access to the implant. The gateway device not only jams wireless communication and blocks transmissions (e.g., from an adversary) from reaching the implanted device, but it also impersonates the implanted device and communicates with an adversary's system whenever it detects an adversary attempting to access the implant. Because all of the adversary's access requests are being received and processed by the external gateway rather than the implant, it is not possible for the adversary to subject the implant to a resource depletion attack and exhaust its battery or otherwise disrupt its functioning by subjecting the implant to an unending series of access requests. In the case of a medical emergency, medical personnel who are treating the device's host need only locate and power off the external gateway device worn or carried by the host; as soon as the gateway has been disabled and its jamming and spoofing activities have ceased, direct wireless access to the implanted will be possible.<sup>38</sup> In a sense, this model is similar to the "Cloaker" approach proposed by Denning et al., however it places no drain on the IMD's battery, since the IMD does not need to send periodic "Are you there?" queries (or otherwise transmit data to) the external component. It also eliminates the possibility that an adversary could impersonate the external cloaking device and send wireless signals to the IMD that force the IMD to remain secured and inaccessible when the device's host is indeed undergoing a health emergency and medical personnel have removed the "real" cloaking device from the host's person.

#### **AUDIBLE ALERTS TO INCREASE HOST'S AWARENESS OF POTENTIAL ATTACKS**

Halperin et al. note that some IMDs generate an audible alert that their host can hear when the device's battery is nearly exhausted, and they recommend that similar audible alerts be used as a supplemental security measure

---

<sup>38</sup> See Zheng et al., "A Non-key based security scheme supporting emergency treatment of wireless implants" (2014).

for IMDs: if a device detects suspicious activity that may indicate an attack (such as a series of unsuccessful attempts by a wireless user to access the device), the device could generate an audible alert that the device's human host would hear.<sup>39</sup> Halperin et al. note that while such an alert would not in itself directly block an ongoing attack against the device, the fact that the device's host has been alerted to the possibility of an ongoing attack means that the host then could take specific actions (e.g., as previously instructed by the device's operator) that would directly prevent or block an attack that was in progress.

However, Hei and Du note that an audible alert might not be noticed by the device's host if the he or she were in a noisy environment (nor, we might add, if the host were asleep); they also note that a mechanism for generating an audible alert consumes electrical power and thus cannot easily be incorporated directly into an implantable device itself, insofar as power is a limited and very precious commodity for many such devices.<sup>40</sup>

Halperin et al. propose to avoid such power constraints by implanting a secondary device whose sole purpose is to audibly alert its human host to attacks on the primary implanted device. They have developed an implantable prototype based on the Wireless Identification and Sensing Platform (WISP) that can harvest energy from an external power source in the form of a radio signal generated by a standard UHF RFID reader; in this way, the secondary WISP device places no demands on the power supply of the primary device implanted in the host.<sup>41</sup> The WISP devices uses a piezoelectric element to generate an audible beep if it detects certain kinds of RF activity (such as a series of wireless access requests from an external RFID reader) that could indicate an attempt by an adversary to access the primary implanted device.

An alternative approach proposed by Halperin et al. similarly relies on the use of sound to make a device's host aware of a potential attack: they have developed a prototype implantable device that exchanges its symmetric cryptographic key with an external system using sound waves that are audible to the device's host and detectable by an external system in close proximity to the host's body but not detectable (e.g., to adversaries) at significant distances from the host's body.<sup>42</sup> In this way, whenever the device's host hears the relevant kind of sound generated by the implanted device, he or she knows that some external system has just submitted an access request to the implanted

<sup>39</sup> See Halperin et al., "Security and privacy for implantable medical devices" (2008), p. 37.

<sup>40</sup> See Hei & Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies" (2011), p. 2.

<sup>41</sup> See Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" (2008).

<sup>42</sup> See Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" (2008).

device and is receiving the cryptographic key. If that attempt is unauthorized, the host could potentially thwart it by moving away from that location and away from whatever external device was the source of the attack.

### **Securing a neuroprosthetic device vs. securing a neurocybernetic device-host system**

A recurring theme throughout this text will be the distinction between ensuring information security for a neuroprosthetic device *per se* and ensuring information security for the larger neurocybernetic system that includes both the device and its human host. When discussing information security for neuroprosthetic devices, one must be careful to clarify whether the goal and effect of a particular security control is to strengthen the security of information contained within the device or within the larger device-host system.

For example, imagine a human being who possesses an advanced cochlear implant that records all of the person's auditory experiences and can later "play back" any part of the recording internally through the person's cochlear nerve in a way that only he or she can hear, with the playback feature activated and controlled by acts of volition within the host's mind.<sup>43</sup> It may be the case that the cochlear implant possesses numerous security controls that make it almost impossible for an unauthorized party to directly access the information stored within it. Such controls might include, for example, an anti-tampering mechanism that destroys the device's internal memory if the device's physical casing is removed and a biometric control integrated into the device's processor that is based on the host's unique cognitive patterns and which disables the playback feature if the device were to be transplanted into some other host's body or physically connected to another computer. In this situation, one might say that all of the recorded auditory information stored on the device's internal memory is (almost) completely secure from access by any unauthorized party. But if we look not at the physical neuroprosthetic device itself but at the larger device-host system of which it is a component, we see that the information stored in the device is in fact highly insecure: the device's host can play back recorded information (such as a conversation that he or she had overheard) in his or her mind through a simple act of will and then easily share that information with unauthorized parties simply by repeating it aloud, writing it down, or answering parties' questions about the information.

---

<sup>43</sup> Regarding the possibility of such playback devices, see Merkel et al., "Central Neural Prostheses" (2007), and Robinett, "The consequences of fully understanding the brain" (2002).

The device's host might share such information with unauthorized parties accidentally and unintentionally (e.g., sharing information about a sensitive conversation without realizing that the person with whom the information was being shared is an unauthorized party), as an intentional action performed by the host (e.g., sharing information from a damaging conversation in order to exact revenge on a disliked coworker), or under duress (e.g., as a result of severe threats, blackmail, or enticement offered by the unauthorized party).

If the developers and operators of neuroprosthetic devices wish to maximally secure information contained within their devices, they must consider not only the characteristics and performance of a device as it exists in the abstract – physically and operationally separated from its human host – but also how the device functions when integrated into the neural circuitry of a particular human host. The device-host system may demonstrate unique cybernetic, biocybernetic, and neurocybernetic characteristics (such as feedback loops and other relationships of communication and control) that are neither visible nor even extant when the device and its host are considered separately or are, in fact, disconnected from one another.

Moreover, we will also extensively consider the possibility that an attack might be launched on a neuroprosthetic device by an adversary not for purposes of compromising information stored within the device itself but for the ultimate purpose of compromising the security of information stored within the natural biological systems and cognitive processes of the device's host (e.g., within the host's memory or conscious awareness) – perhaps by undermining his or her health or safety. There is also a possibility that an adversary could render information stored on a neuroprosthetic device damaged, disclosed, or inaccessible not by directly attacking the device but by launching an attack (whether by biochemical, physical, psychological, or other means) against the device's human host.

### **The weakest link – now at the heart of an information system**

Human beings are considered to be the weakest link in any system of information security controls:<sup>44</sup> not only can we make unintentional physical or mental errors in operating a system or be fooled by social engineering attacks,

---

<sup>44</sup> See Sasse et al., "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security" (2001); Thonnard et al., "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat" (2012); and Rao & Nayak, *The InfoSec Handbook* (2014), pp. 307-23.

we can also potentially become corrupted through greed, jealousy, resentment, lust, shame, pride, or ambition, and agree to take on an active and intentional role in disabling or bypassing our organization's security controls.<sup>45</sup>

With some kinds of information systems – e.g., those that are housed in physically and electronically isolated environments; are managed by a small and carefully screened team of expert personnel; contain no information that is financially, politically, or personally sensitive; and, once activated, perform their tasks in an automated manner largely devoid of direct human intervention or control – the opportunity for security vulnerabilities to be intentionally exploited by human adversaries or unintentionally triggered by human agents can be reduced to a relatively small level. With other kinds of systems that have a much higher exposure to human activity – such as systems that are physically housed in publically accessible or mobile locations; have hundreds or thousands of individuals who possess privileged access to the system; and contain highly sensitive and valuable information that is provided, altered, and deleted daily by millions of human users utilizing web-based interfaces – the threat that a system's information security will eventually be compromised by human agents acting intentionally or unintentionally can be much greater.

It is easy to see that in the case of advanced neuroprosthetic devices, a system will always possess a large and crucial human element that cannot be eliminated: namely, the fact that the device is actually integrated into the neural circuitry of a human being. In this sense, a neuroprosthetic device inherently demonstrates a unique set of vulnerabilities that are found in no other systems, whether they be supercomputers, desktop computers, laptops, mobile or wearable devices, ubiquitous computing devices in smart homes or offices, web servers, automobiles, robotic manufacturing systems, communications satellites, video game systems, or any other computerized systems or devices.

The human mind – with its emotions, cognitive biases, incomplete knowledge, uneasy mix of gullibility and suspicion, and unique values and motivations – forms a perilous and unpredictable element of any information system. And in the case of an advanced neuroprosthetic device, that mind is often permanently anchored at the very heart of the system, where it is relentlessly active 24 hours a day in influencing and perhaps even controlling the functioning of the system – where it may be able to bring about some dramatic change in the contents of an information system or some tangible

---

<sup>45</sup> For the possibility of insider threats, see Coles-Kemp & Theoharidou, "Insider Threat and Information Security Management" (2010).

physical action in the world simply by means of an idle thought or volition or the recalling of a hazily outlined memory.

Many kinds of advanced neuroprosthetic devices take the most dangerous and weakest possible link and embed it irrevocably at the very core of an information system which one nevertheless hopes to – somehow – make secure. Admittedly, this intimate connection between mind and machine can also possess its own unique advantages. The human mind tied to a neuroprosthetic device can display human strengths such as flexibility, intuition, the ability to correlate vast and unrelated pieces of knowledge and experience, creativity, and even faith, hope, and love – characteristics that allow a human mind not only to detect threats that a machine may be unable to recognize but also to wisely discern those rare instances when bypassing, disabling, or ignoring a security control in some particular circumstance may actually be the best (or only) way to ensure the information security of a system, individual, or organization. From the perspective of information security, integrating the neural circuitry of a human being with an electronic device can – for better or worse (or both) – bring with it not only the neurons and synapses of a human brain but also the intellectual, emotional, and even spiritual aspects of a human mind.

### **New kinds of information systems to be protected – or used in executing attacks**

Information security experts whose goal is to develop and implement mechanisms and procedures to ensure the information security of advanced neuroprosthetic devices and their corresponding device-host systems have a clear need to learn as much as possible about the capacities and uses of advanced neuroprosthetic devices. What may be less immediately obvious is that *all* information security practitioners may need to develop at least some basic knowledge or awareness of the capacities and uses of advanced neuroprosthetic devices, insofar as such technologies provide powerful new tools by means of which attacks against all kinds of information systems – whether laptop computers, web servers, smartphones, archives of printed documents, or even human minds – can be launched and executed by sufficiently skilled adversaries.

Some adversaries may operate neuroprosthetic devices that are implanted in their own bodies. For example, a person could use an artificial eye to record secret video, an advanced cochlear implant to record conversations that are scarcely audible to a normal human ear, or an advanced virtual reality neuroprosthetic that allows him or her operate within cyberspace, sensing and manipulating it in a way that no unmodified human being could. Other adversaries might not host any neuroprosthetic devices within their own bodies,

but they might be able to gain unauthorized access to neuroprosthetic devices implanted in other human hosts. For example, an adversary who hacked into the artificial eye of a corporation's vice president might use the ongoing live video feed to gain access to a plethora of financially valuable business secrets that are displayed on the vice president's computer screen and are contained in a corporate computer system that is otherwise impossible to break into. An adversary could gain access to a secured facility not by tunneling into the building but by hacking into the human security guard's mnemoprosthetic implant and creating a false memory of the "fact" that the adversary is a senior staff member at the facility and should be welcomed when he arrives at the front door.

In such ways, the use of advanced neuroprosthetic devices within human societies will require not only the development of a specialized subfield of information security dedicated to securing such devices and their device-host systems but also new approaches and responses across all of the other subfields of information security, as they adapt to the existence of such new technological means for planning and executing attacks on information systems.

### New possibilities for biometrics

Other researchers have suggested that one approach to creating implantable devices that are highly secure during normal circumstances but grant open access during health emergencies is to take advantage of one of the unique strengths of implantable devices: namely, their ability to draw rich, real-time biometric data from their human host. Biometrics that have been used for purposes of authentication for information systems in general (but not implantable neuroprosthetic devices in particular) include:<sup>46</sup>

- Facial geometry
- Ear geometry
- Hand geometry (including vascular patterns)
- Fingerprints
- Palmprints
- Retinal patterns
- Iris patterns
- Infrared thermograms of patterns of heat radiated from the face or hand

---

<sup>46</sup> See Delac & Grgic, "A Survey of Biometric Recognition Methods" (2004), and Rao & Nayak, *The InfoSec Handbook* (2014), pp. 297-303.

- Signature and handwriting patterns
- Keystroke and typing patterns
- Gait and walking patterns
- Vocal characteristics
- Odor
- DNA

Many of these biometrics may be impractical if the designer of a neuroprosthetic device is attempting to create a security control mechanism within the device to ensure that it is still located within and being operated by its intended human host. For example, a memory implant located within its host's brain has no direct means by which to observe the iris patterns or patterns of heat radiated from the hands of its human host. However, an implanted neuroprosthetic device could potentially utilize some such biometrics if it had access to relevant biological sensory systems within its host: for example, if a sufficiently sophisticated neuroprosthetic device implanted within its host's brain had access to the optic nerve or visual cortex, it could conceivably conduct an iris scan by asking its host to stand in front of a mirror and look at the reflection of his or her own eyes. Instead of verifying that a neuroprosthetic device is still implanted in its intended host, some such biometrics could potentially be used by a neuroprosthetic device to authenticate another individual (such as a maintenance technician) who is not the device's host but who is an authorized user and who should be given access to the device's systems: for example an individual who possesses a bidirectional robotic prosthetic arm could potentially authenticate that another person is an authorized user simply by shaking the person's hand and thus detecting the person's hand geometry through touch or through optical or thermal sensors embedded in the prosthetic hand's palm or fingers.

Beyond such general-purpose biometrics, a number of biometrics have been developed or considered especially for use with implantable medical devices and are designed to take advantage of an implanted device's ability to directly access information about its host's internal biological processes. Such biometrics include:<sup>47</sup>

- Heart rate
- Breathing rate
- Blood glucose level
- Hemoglobin level

---

<sup>47</sup> See Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), pp. 207-09.



- Body temperature
- Blood pressure

Below we consider a number of biometrics and biometric systems that have been specifically proposed for or could conceivably be applied for use with advanced neuroprosthetic devices.

#### **FINGERPRINT TYPE, EYE COLOR, HEIGHT, AND IRIS PATTERN**

Hei and Du have proposed a biometric-based two-level security control to allow medical personnel to access implantable medical devices during an emergency. Prior to its implantation, a key is installed on an IMD that contains information about the basic fingerprint type, eye color, and height, and a code representing the iris pattern of its human host. When emergency medical personnel attempt to remotely access the IMD using their computer, the device will first ask the personnel to enter the host's fingerprint type, eye color, and height, as an initial access control; the medical personnel can obtain all of this information by physically observing and manipulating the host, even if he or she is unconscious. As a more sophisticated control, the IMD then asks the medical personnel to take a photo of the host's iris (e.g., with a smartphone); an algorithm uses the photo to generate a code representing the iris pattern, which is then compared against the host's reference iris code stored in the IMD.<sup>48</sup>

Hei and Du note that such an approach would fail to provide access to legitimate medical personnel, for example, in cases in which the host's fingerprints had been damaged due to a fire or other injury or in which the host's body was trapped or positioned in such a way that the personnel could not photograph the host's eyes.

Another possible disadvantage of this approach is the fact that it is based on the presumption that authorized emergency medical practitioners are the only individuals who would have both the desire to access and control the host's IMD and the ability to gather the necessary biometric data through direct physical interaction with the host. However, it seems possible that a sufficiently motivated adversary who wishes to gain unauthorized access to the host's IMD could potentially gather all of the needed biometric data simply by downloading high-quality images of the individual from the Internet.<sup>49</sup>

---

<sup>48</sup> See Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012), p. 208.

<sup>49</sup> For an example of this sort of vulnerability and risk, see Hern, "Hacker fakes German minister's fingerprints using photos of her hands" (2014).

### THE HEART'S INTERBEAT INTERVAL

Cho and Lee propose a model for secure communication among implanted biosensors or between an implanted biosensor and external system that uses the interbeat interval of the host's heartbeat.<sup>50</sup> The advantages of using that data source as a symmetric key for secure communications include the heartbeat's relatively high level of randomness (in comparison to some other potential biometrics) and the fact that the heart's interbeat interval can be detected by devices located throughout the host's body using a variety of mechanisms (e.g., by registering electrical activity or blood pressure) and can also be detected on the external surface of the host's body but cannot easily be detected by any adversary who does not have direct physical access to the host at that moment.

### STRINGS GENERATED FROM REAL-TIME ECG SIGNALS

Zheng et al. propose an "ECG-based Secret Data Sharing (ESDS) scheme" to secure information that is being transmitted from an implanted device to an external system. Before its transmission from the implanted device, data is encrypted by the device using a key based on current biological activity that generates ECG signals that the device registers and which an external ECG is also capable of recording. After the message has been transmitted, it can be decrypted by an external system that had been using its own external ECG unit to record the host's activity at the same time and which can thus reconstruct the key.<sup>51</sup>

### GAIT AND VOICE PATTERNS

Vildjiounaite et al. propose a noninvasive multimodal model for securing personal mobile devices such as smartphones<sup>52</sup> that in principle could also be applied to implantable neuroprosthetic devices. Their approach involves utilizing a device's built-in microphone and accelerometer to gather information about both the unique gait or walking patterns of the device's host along with unique characteristics of the host's voice. After activation, the security program enters a "learning mode" for a period of a few days, during which time it records and analyzes the host's typical gait and voice patterns; if the device is able to establish suitably stable reference patterns, it then enters the "biometric authentication mode" in which it regularly compares the

---

<sup>50</sup> See Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012).

<sup>51</sup> See Zheng et al., "Securing wireless medical implants using an ECG-based secret data sharing scheme" (2014), and Zheng et al., "An ECG-based secret data sharing scheme supporting emergency treatment of Implantable Medical Devices" (2014).

<sup>52</sup> See Vildjiounaite et al., "Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices" (2006).

gait and voice patterns that it is currently detecting against the reference patterns stored within it and – assuming that the current patterns and reference patterns match – authenticates the device’s host and provides ongoing access to services.<sup>53</sup>

### **BEHAVIOR CHANGES**

Denning et al. note that one approach to securing implantable medical devices involves “patient behavior changes,” in which the host of a device is asked to modify his or her behavior in some way as part of implementing a security control.<sup>54</sup> The sense in which Denning et al. use the phrase is broad enough to include cases in which the host’s behavior change is the result or side-effect of a security control rather than the primary means by which the control is enforced. However, momentary “behavior changes” could also be used as a sort of security control to verify that a neuroprosthetic device was still being used by its intended human host. For example, a device’s host might periodically receive a certain kind of signal from the device, such as a visual alert displayed in the host’s field of vision, an auditory alert produced through stimulation of the auditory cortex that the host can hear but no external parties can detect, or a stimulation of the host’s proprioceptive system. After receiving the signal, the host then has a limited period of time in which to perform some particular (ideally inconspicuous) behavior that the implanted device can detect – such as blinking his or her eyes in a certain pattern, making a certain sound, or moving his or her fingers in a particular way. If the device detects the required behavior, it authenticates the device’s host as an authorized party and allows ongoing access to the device’s services for a particular period of time.

### **THOUGHTS AND MEMORIES**

One model of using a user’s thoughts and memories as a biometric is presented by Thorpe et al. in their proposed mechanism for utilizing “pass-thoughts.” In the simplest such approach, an authorized user memorizes a brief password, thereby storing it as a memory within his or her mind. When the user wishes to access a system, the system displays a random sequence of highlighted letters, and whenever the highlighted character happens to be the next character in the user’s password, the user’s brain generates a P300 potential spike (or a positive potential that occurs roughly 300 milliseconds

---

<sup>53</sup> Vildjiounaite et al., “Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices” (2006), p. 197.

<sup>54</sup> Denning et al., “Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010) p. 919.

after the notable event) that can be detected by the system using an EEG or other device. Thorpe et al. note that such a pass-thought need not involve a text string; it could alternatively involve the use of “pictures, music, video clips, or the touch of raised pin patterns” or anything else that a person is capable of remembering and which the system is capable of displaying or presenting.<sup>55</sup> However, at its heart such a “pass-thought” mechanism is essentially based on the use of a password as traditionally understood; the main difference is that rather than typing the password on a keyboard or speaking it aloud, an authorized user “enters” the components of the password through interaction with a brain-computer interface that utilizes a device such as an EEG. Such a system thus displays many similarities with traditional password-based systems, insofar as an authorized user might forget his or her pass-thought (e.g., if it had been a long time since the user had last attempted to access the system); similarly, a user could be issued a new temporary pass-thought by a system’s administrator (e.g., by displaying the contents of the pass-thought on a screen and asking the user to remember it) and the user could change the pass-thought to something new of his or her own choosing.

One can imagine other more sophisticated kinds of security controls based on cognitive processes such as thought and memory that are more exotic and which from an operational perspective have less in common with traditional password-based systems. For example, the same word (e.g., “home” or “mother” or “cat”) or image (e.g., that of a wooded lake or a birthday cake) displayed to different individuals will generate different associations and the recall of different memories within each of the individual’s mind because of the unique contents of each person’s memories and life experience. The contents and internal interrelationships of such mental semantic networks could potentially be used as a form of authentication that cannot easily be lost, stolen, or spoofed, insofar as they are not directly accessible to parties outside of the mind that possesses them, and a human being cannot adequately understand and describe the nature and contents of his or her mental semantic networks even if he or she were intentionally attempting to do so (e.g., because the person were being subjected to threats or blackmail).

## **DNA**

The use of DNA for verifying the identity of individuals has traditionally been limited to forensic applications rather than biometric access control for information systems, due to the fact that technologies have not yet been developed allowing simple real-time analysis and matching of a DNA sample with a reference pattern; however if such technologies were to someday be developed, DNA could potentially prove to be the most reliable of all biometrics (with some rare limitations, such as the case of identical twins whose

---

<sup>55</sup> See Thorpe et al., “Pass-thoughts: authenticating with our minds” (2005).

DNA is indistinguishable).<sup>56</sup> Because of the uniqueness of DNA and its potentially high reliability as a biometric, some information security experts have suggested that it could someday be utilized as a biometric means for an implanted neuroprosthetic device to verify that it is operating within its intended human host.<sup>57</sup>

Spurred by ongoing advances in bionanotechnology, biomolecular computing, and related fields, DNA could also someday be used as a biometric or authenticator in other ways. For example, in the case of a neuroprosthetic device that is composed of synthetic biological materials, other implanted systems could analyze the device's DNA in order to verify its origins and authenticate it (e.g., locating a particular sequence of DNA within the device's genetic material in order to confirm that the device was created by the intended authorized manufacturer and was not an unauthorized growth or biohack that had somehow been cultivated within the device's host through an adversary's introduction of engineered viruses, surgical nanorobots, or other unauthorized agents).

Multiple devices that have been implanted in the same host and which form a system could also potentially communicate with one another through their production of different viruses or biological material that are released into the host's bloodstream and travel between devices, e.g., utilizing the engineered virus's DNA or RNA as a data-storage mechanism for transmitting messages between the implanted devices and allowing one device to verify that the other devices are still present and functioning within the host's body. An electronic or biological neuroprosthetic device could also use DNA, for example, as a means of deploying and storing encryption keys for use in authenticating or being authenticated by other systems.<sup>58</sup>

### **ORGANISMIC CONTINUITY (OR A CONTINUAL "LIVENESS SCAN")**

Qureshi notes that some kinds of biometric traits can be spoofed by presenting the biometric reader with an artificial construct of some sort that is not actually part of the authorized party's living organism but which nonetheless presents patterns that mimic those of the person's organism.<sup>59</sup> Thus some kinds of fingerprint readers could potentially grant access to an adver-

---

<sup>56</sup> Delac & Grgic, "A Survey of Biometric Recognition Methods" (2004), p. 188.

<sup>57</sup> For example, the question of whether this might be a feasible approach has been posed by Pająk (2015).

<sup>58</sup> For a discussion of the possibilities of using DNA as a mechanism for the storage of data, see Church et al., "Next-generation digital information storage in DNA" (2012).

<sup>59</sup> See Qureshi, "Liveness detection of biometric traits" (2011).

sary if the adversary presented a silicon “finger” whose surface texture replicated the fingerprint pattern of an authorized user, and some kinds of iris scanners could potentially be fooled if presented a high-quality photograph of an authorized user’s iris. Qureshi notes that one way to prevent such spoofing is to incorporate mechanisms for “liveness detection” which verify that the presented biometric was actually being generated by a living organism.

For example, adding pulse and moisture detection capabilities to a fingerprint scanner can help the scanner to ensure that a presented biometric is being provided by a living finger and not a rubber replica, and an iris scanner could instruct its user to blink at certain moments, which induce predictable changes in the size of a living iris but not in a photographic replica.<sup>60</sup>

While helpful, such liveness detection is not foolproof. Even if an adversary were to possess sufficiently sophisticated genetic engineering and bioengineering technologies, it would generally not be possible for an adversary to directly “grow” a living organ or body part capable of fooling a biometric scanner: for example, it is not possible to generate a replica of a human being’s fingerprint or iris pattern simply by obtaining a sample of the person’s DNA and attempting to culture a cloned finger or eyeball, since an individual’s fingerprints and iris patterns are shaped by many environmental factors beyond simple genetics. However, if the details of an authorized user’s fingerprints or iris pattern were known, a living replica could perhaps be created through other means – such as using a combination of nanotechnology and biotechnology to sculpt, reshape, or otherwise reengineer the finger or iris of an unauthorized living being so that its visible patterns sufficiently matched those of the authorized target.

However, in principle the concept of liveness detection could be applied to prevent such attacks and ensure that an implanted neuroprosthetic device is not only being accessed by *a* living being who displays certain characteristics but that it is being accessed by *the same living being* in whom it was originally implanted. For example, imagine that immediately upon its implantation in a human host, a neuroprosthetic device begins a continual, ongoing “liveness scan” designed to ensure that the device is implanted in a living host – for example, by monitoring brain activity. As long as the process of scanning is reliable and uninterrupted, then as long as the scan has shown that from the moment of the device’s implantation up to the present moment the monitored biological activity has continued without ceasing, then the device’s software could be confident that the device is not only implanted within some living organism but within the organism of its original human host.<sup>61</sup>

---

<sup>60</sup> Qureshi, “Liveness detection of biometric traits” (2011), pp. 294-95.

<sup>61</sup> Such a model assumes that extracting the implant and transferring it to another living host

Such a biometric security control based on the detection of “organismic continuity” could be used, for example, to automatically disable – or delete the stored contents of – an implanted neuroprosthetic device upon the death of its human host or the cessation of particular brain activity within the host. Care would need to be given to the design of such systems to ensure that a neuroprosthetic device did not erroneously deactivate itself and cease to operate in cases in which its host had, for example, suffered a heart attack or stroke or entered a coma when such a termination of functionality was not the intention of the device’s designer, manufacturer, or operator.

### **Nontraditional computing platforms: from biomolecular computing and neural networks to nanorobotic swarms**

When compared to conventional information systems such as desktop computers, laptops, and smartphones, an advanced neuroprosthetic device may be more likely to possess nonstandard, non-electronic components and to utilize nontraditional computing processes and formats. In the case of conventional computers, there is a decades-long history of design ingenuity, trial, error, and consumer feedback that has generated a body of experience and best practices allowing the efficient development and manufacturing of very powerful devices that utilize technologies such as silicon-based microprocessors, nonvolatile memory based in magnetic discs or flash memory, and computer programs constituting sets of instructions that can be loaded and executed by a central processing unit.

When developing new mass consumer electronics devices, it often makes more business sense for manufacturers to keep the cost and complexity of manufacturing processes at a minimum by designing devices that utilize well-established computing technologies while simultaneously attempting to advance those computing technologies in a way that enhances existing performance and capacities in an incremental manner. When designing a next-generation mass-market smartphone intended for consumer release next year, it would most likely be seen as an unnecessarily exotic (and practically and economically unfeasible) approach for a manufacturer to attempt to build the device’s internal computer on a platform utilizing as biomolecular computing, quantum computing, or physical neural networks.

---

could not be accomplished without at least a momentary break in the relevant recorded biological activity by the device; it also assumes that the device’s design and structure are such that the recorded biological activity must actually be generated by biological activity occurring in biological material directly adjacent to the device and not, for example, spoofed through a targeted wireless transmission of certain electromagnetic radiation.

Advanced neuroprosthetic devices, on the other hand, already inherently incorporate and rely on at least some highly “exotic” and “nonstandard” computing components and processes, insofar as they must integrate both physically and operationally with the biological structures and neural circuitry of their human host. When considering information security for advanced neuroprosthetic devices, one cannot assume that a neuroprosthetic device will be a traditional computing device – with traditional kinds of components, architectures, memory systems, and ways of gathering and processing information to generate actions and output – that has simply been implanted into the body of a human host.

While some advanced neuroprosthetic devices might indeed resemble a smartphone that has just been miniaturized and implanted in a human body, other neuroprosthetic devices might scarcely be recognizable as computers – or even technological devices. Neuroprosthetic devices that perform the processing of information by means of a physical neural network might be partially or fully constructed from biological materials and may be integrated into the body of their host in a way that makes it difficult to discern – both structurally and operationally – where the host ends and the device begins. Information security might involve protecting a neuroprosthetic device not only against computer viruses but against biological viruses, as well. In order to avoid invasive surgery that could damage a human host’s brain, other neuroprosthetic devices might consist of a swarm of nanorobots that have been designed to be capable of crossing the blood-brain barrier and which are introduced into the host’s bloodstream and find their way to the correct location in the brain, where they work together to stimulate (or are stimulated by) the brain’s natural interneurons in particular ways, even while retaining their physically diffuse structure.<sup>62</sup>

The possibility that neuroprosthetic devices might take such forms creates unique issues and considerations for information security. On the one hand, the use of nontraditional components, structures, and computing methods may render a neuroprosthetic device more secure, because common kinds of attacks that are often effective against conventional computers and information systems may be ineffective or even wholly inapplicable in the case of neuroprosthetic devices. On the other hand, the use of nontraditional elements may mean that the designers, manufacturers, operators, and hosts of neuroprosthetic devices cannot rely on the vast body of information security knowledge and best practices that have been developed over decades for securing conventional computer systems, because many of those information security strategies, mechanisms, and techniques may also be ineffective or inapplicable in the case of neuroprosthetic devices.

---

<sup>62</sup> See Al-Hudhud, “On Swarming Medical Nanorobots” (2012).



## Technology generating posthuman societies and posthuman concerns

Philosophers of technology have given much thought to the transformative effects that technology can play in the lives of human beings, either as a means of liberation and self-fulfillment or as a source of oppression and dehumanization.<sup>63</sup> Even technologies such as desktop computers and email – which interface with the human mind in only limited and indirect ways – have resulted in major psychological, social, and cultural impacts among the human beings who use them.<sup>64</sup> However, advanced neuroprosthetic devices have the potential to reshape human psychological, social, and cultural realities – and even challenge many popular notions of what it means to be “human” – in ways greater and more powerful than those demonstrated by previous generations of technology. In this regard, advanced neuroprosthetics are similar to other technologies such as genetic engineering, artificial intelligence, social robotics, virtual reality, and nanotechnology that have the potential to reshape human existence in such a way that the resulting kinds of beings, systems, and organizations might best be described as “posthuman.”<sup>65</sup>

Already “cyborg-cyborg interaction” is becoming a fundamental aspect of society,<sup>66</sup> and genetic engineering may accelerate trends of cyberization by further enhancing the ability of the human body to interface at a structural level with implanted or external technological systems. Increasingly businesses and other organizations comprise “cybernetic teams” whose human and artificial members “cooperate as teammates to perform work.”<sup>67</sup> Indeed,

---

<sup>63</sup> For a discussion of such questions in the context of human augmentation and neuroprosthetics, see Abrams, “Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault” (2004); Kraemer, “Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation” (2011); Erler, “Does Memory Modification Threaten Our Authenticity?” (2011); Tamburrini, “Brain to Computer Communication: Ethical Perspectives on Interaction Models” (2009); and Schermer, “The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction” (2009).

<sup>64</sup> For example, see Fox & Rainie, “The Web at 25 in the US: Part 1: How the Internet Has Woven Itself into American Life” (2014), and Shih, “Project time in Silicon Valley” (2004).

<sup>65</sup> For the convergence of nanotechnology, biotechnology, information technology, and cognitive science (or “NBIC” technologies), see Gordijn, “Converging NBIC Technologies for Improving Human Performance” (2008); for a deeper exploration of such technologies’ relationship to posthumanism and posthumanity, see Birnbacher, “Posthumanity, Transhumanism and Human Nature” (2008). For aspects of posthumanism that extend beyond technology, see Miah, “A Critical History of Posthumanism” (2008).

<sup>66</sup> See Fleischmann, “Sociotechnical Interaction and Cyborg–Cyborg Interaction: Transforming the Scale and Convergence of HCI” (2009).

<sup>67</sup> See Wiltshire et al., “Cybernetic Teams: Towards the Implementation of Team Heuristics in HRI” (2013); Bradshaw et al., “From Tools to Teammates: Joint Activity in Human-Agent-Robot

the increasing virtualization of our relationships means that we will regularly interact with coworkers, customers, and suppliers as digital avatars in virtual environments, without knowing (or perhaps caring) whether the entity on the other end of a conversation is a human being, social robot, or AI program.<sup>68</sup> Neuroprosthetics will allow for increasingly intimate forms of communication that do not involve physical face-to-face interaction but are instead mediated by technology, thereby facilitating the development of new kinds of posthuman interpersonal relationships and social structures.<sup>69</sup>

Such powerful new technologies are introducing a “radical alterity” that challenges not only the traditional values of humanism but also our most fundamental understanding of the limits and possibilities of what it means to be human, in a time when philosophical and ethical frameworks that “privilege reason, truth, meaning, and a fixed concept of ‘the human’ are upended by digital technology, cybernetics, and virtual reality.”<sup>70</sup> A variety of responses to such technologies has emerged. For example, on the one hand, scientists and philosophers identifying themselves as **transhumanists** accept the basic humanistic principles of anthropocentrism, rationality, autonomy, progress, and optimism about the future of humanity, while actively working to employ science and technology in an effort to control and accelerate the transformation of the human species in ways that traditional biological evolution does not allow. Such thinkers advocate the use of genetic engineering, cybernetics, and nanotechnology to create a supposedly more meaningful, more transcendent, “enhanced” form of human existence. In this sense, their philosophy can be understood not as “anti-humanism” but as their expression of a unique form of “ultra-humanism.”<sup>71</sup>

On the other hand, there is a diverse group of **posthumanistic** thinkers who agree that new forms of sentient and sapient existence are emerging, spurred on by the world’s technological advances; however, these thinkers reject transhumanism’s anthropocentric and humanistic focus. Instead, posthumanists argue that the future will include many different sources of intelligence and agency that will create meaning in the universe through their networks and relations:<sup>72</sup> such entities might include “natural” human beings,

---

Teams” (2009); and Flemisch et al., “Towards a Dynamic Balance between Humans and Automation: Authority, Ability, Responsibility and Control in Shared and Cooperative Control Situations” (2012).

<sup>68</sup> See Grodzinsky et al., “Developing Artificial Agents Worthy of Trust...” (2011).

<sup>69</sup> See Fleischmann, “Sociotechnical Interaction and Cyborg–Cyborg Interaction: Transforming the Scale and Convergence of HCI” (2009), and Grodzinsky et al., “Developing Artificial Agents Worthy of Trust...” (2011).

<sup>70</sup> See Gunkel & Hawhee, “Virtual Alterity and the Reformatting of Ethics” (2003).

<sup>71</sup> See Ferrando, “Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations” (2013).

<sup>72</sup> See Ferrando, “Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New

genetically engineered human beings, human beings with extensive cybernetic and neuroprosthetic augmentation, human beings who spend most or all of their time dwelling in virtual realities, social robots, artificially intelligent software, nanorobot swarms, and sentient networks.

Thinkers like Bostrom<sup>73</sup> are generally enthusiastic about the transhuman potential of technologies like advanced neuroprosthetics to “liberate” humanity, allowing us to transcend our previous physical and cognitive limitations and spark the evolution of higher forms of human existence. Following paths pioneered by Habermas and Horkheimer, other scholars are more pessimistic about the anticipated impact of such transformative technologies, suggesting that while the exact impact of such technologies cannot be predicted in advance, they are more likely to spur social fragmentation and inequality, a reduction in human autonomy and meaning, and the oppression – or in its extreme form, even destruction – of humanity at the hands of its technological creation.<sup>74</sup>

In a sense, then, questions about the information security of advanced neuroprosthetic devices and device-host systems should be considered in a broader context relating to human societies and the human species: advanced neuroprosthetic devices should be developed (or, if necessary, *not* developed) in such a way that will ensure not only that individual persons’ information security can be protected – but that a humanity and human species can continue to exist whose members are able to generate, use, and exchange information and hope for the protection of its security.

### **Human autonomy, authenticity, and consciousness: risk management and the possibility of ultimate loss**

---

Materialisms: Differences and Relations” (2013).

<sup>73</sup> See Bostrom, “Why I Want to Be a Posthuman When I Grow Up” (2008).

<sup>74</sup> As Abrams has noted, yet another group of thinkers takes an extreme position, arguing that while humanity’s twilight and replacement by artificial beings such as social robots or artificial superintelligences is indeed inevitable, it is in fact a natural and desirable step in the evolution of intelligent life on earth. See Abrams, “Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault” (2004), and Edgar, “The Hermeneutic Challenge of Genetic Engineering: Habermas and the Transhumanists” (2009). The struggle between those who wish to build a utopian world and manipulate the very nature of reality through the technological augmentation of human beings and those who shun such technologies and instead wish to build a utopia and reshape reality by means of a spiritual or mystical “augmentation” of human beings is a theme that has been well explored within literature, film, and popular culture. For an analysis of one such dichotomy, see Szczepocka, “Konflikt sprzecznych utopii jako główny problem gry fabularnej ‘Mag: Wstąpienie’” (2015).

Advanced neuroprosthetics thus force us to ponder the future existence and nature of humanity in a way that is elicited by other technologies such as nuclear weaponry or genetic engineering but is not found, for example, with technologies such as desktop computers or even self-driving automobiles. Nevertheless, from the perspective of information security, the primary focus with regard to advanced neuroprosthetic devices is typically very much the technology's impact on and use by particular human beings. And through their interaction with a human being's neural circuitry, many advanced neuroprosthetic devices have the potential to reshape and transform an individual life in ways that are incredibly powerful – and can be either beneficial or harmful.

One of the gravest (and most unique) concerns that an information security professional must consider with regard to neuroprosthetic devices is the impact that they might have on the autonomy, authenticity, and conscious awareness of their human host.<sup>75</sup> Researchers have found, for example, that some human beings who have utilized neuroprosthetic devices for deep brain stimulation in order to treat conditions such as Parkinson's disease have reported feelings of reduced autonomy and authenticity: some such individuals find it impossible to know any longer whether "they" are actually the ones responsible for their thoughts, desires, emotions, and decisions, or whether these mental phenomena are being influenced, controlled, or even created by the electrodes firing deep within their brains.<sup>76</sup>

It is possible to imagine a concrete outcome of the use of particular kinds of (poorly designed or implemented) neuroprosthetic devices which – from the perspective of their human hosts – would produce not only harm but the

---

<sup>75</sup> For an exploration of the ways in which the implantation and use of advanced neuroprosthetic devices (and the accompanying process of "cyberization" of the devices' human hosts) can contribute to a new form of personal identity for a device-host system that fuses both biological, cultural, and technological elements, see Kłoda-Staniecko, "Ja, Cyborg. Trzy porządki, jeden byt. Podmiot jako fuzja biologii, kultury i technologii" (2015). For a discussion of the significance of the physical boundaries of a human organism and the ways in which technologies such as implantable neuroprosthetics can impact cognitive processes and the "moral sense of person" vs. "the notion of person as a subject of experiences," see Buller, "Neurotechnology, Invasiveness and the Extended Mind" (2011). For a philosophical analysis of "threats to personal autonomy" posed by brain-machine interfaces, see Lucivero & Tamburrini, "Ethical Monitoring of Brain-Machine Interfaces" (2007). Questions of personal identity and authenticity are explored by Schermer, "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction" (2009).

<sup>76</sup> See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011), and Berg, "Pieces of Me: On Identity and Information and Communications Technology Implants" (2012). It should be noted that Kraemer explains that other users of neuroprosthetics for deep brain stimulation report precisely the opposite experience: they feel as though the neuroprosthetic devices have *restored* their autonomy and given them increased authenticity as – for the first time in years – they are in control of their bodies once again.

termination of their personal identity and annihilation of their existence as a human subject within the world. For example, a mnemoprosthetic implant that is designed to enhance its users' memory capacities but which causes many of its users to enter a coma or vegetative state would be legally and ethically impermissible – not to mention being counterproductive from an information security perspective, insofar as it would render the information contained within a user's mind unavailable even to that user himself or herself.

Arguably, though, an even worse scenario would be that of a neuroprosthetic device that permanently destroys the autonomy, consciousness, personal identity, continuity of sapient self-awareness, and metavalitionality (or conscience) of its human host – in other words, that obliterates the “essence” of what makes the person human – but that does so in such a way that this destruction is not detectable to other human beings.

For example, consider an extremely sophisticated neuroprosthetic device consisting of a vast network of nanorobotic components that occupy interstitial spaces within the brain and are designed to support the synaptic activity of individual neurons.<sup>77</sup> Imagine that – in a manner that may not be recognized or understood even by the device's designers – this neuroprosthetic device does not actually “support” the natural synaptic activity of the brain's biological neurons but instead controls or replaces it. The physical synaptic connections between neurons (and thus their communication) are disrupted and replaced by connections between the nanorobotic “pseudoneurons.” The person's physical body can still react to environmental stimuli, walk, smile, and even engage in meaningful conversations with family or friends – but in fact, the person's conscious awareness has been eliminated and the person has undergone a sort of “brain death;” all of the outward physical activity is simply being orchestrated by the extremely sophisticated processes of the artificial neural network or computer program that controls the nanorobotic system and which causes it to stimulate particular motor neurons at a particular time in order to generate desired motor behaviors. In effect, the person's body has become a sort of neurocybernetic “zombie,” a mindless puppet controlled by the puppeteer of the neuroprosthetic device.<sup>78</sup>

---

<sup>77</sup> Such technologies have been proposed by some transhumanists as a possible path toward “mind uploading.” See Koene, “Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation” (2012); Proudfoot, “Software Immortals: Science or Faith?” (2012); Pearce, “The Biointelligence Explosion” (2012); Hanson, “If uploads come first: The crack of a future dawn” (1994); and Moravec, *Mind Children: The Future of Robot and Human Intelligence* (1990) for a discussion of such issues from various perspectives.

<sup>78</sup> Gladden, “Tachikomatic Domains: Utopian Cyberspace as a ‘Contingent Heaven’ for Humans,

There are some transhumanists (e.g., proponents of the idea of “mind uploading”) who might argue that such a device would not truly destroy the consciousness or essence of its human host – and that even if it did, they would be willing and even eager to transform their own bodies through the use of such a device, insofar as it might provide a bridge that would allow them to “transfer” their memories and patterns of mental activity into a robotic or computerized body that would essentially allow them, as they see it, to live forever. There may indeed be some human beings who would be happy to imagine that at the cost of destroying their own embodied consciousness, a biomechanical automaton or robot could be created that would go about its activities in the world, replicating the habits and behaviors and continuing the social relationships of the person who had served as its template, simulating the person’s emotions and recreating his or her memories in the way that a video recording recreates some filmed event. But for most human beings, a neuroprosthetic device that destroys their embodied conscious awareness would be considered an absolutely impermissible – and, indeed, lethal – outcome, regardless of whatever other effects it might yield.

A dilemma for information security professionals (and the designers and operators of neuroprosthetic devices) is that in principle it may sometimes be impossible to know what effect a neuroprosthetic device is truly having on the cognitive processes – and especially, on the lived conscious experience – of its human host. If the human host of an experimental neuroprosthetic device asserts that the implantation and activation of the device has in no way harmed or diminished his or her sapience and conscious awareness, this could mean that the device has indeed had no such effect – or that it has destroyed or “imprisoned” the host’s conscious awareness and agency in such a way that the source behind that statement was not the human being but the agency of the neuroprosthetic device itself. It is possible to imagine a situation in which the conscious awareness and autonomous agency of the human host might still exist – but no longer has the ability to control the motor systems of its body and alert the outside world to the fact that it still exists and is essentially “trapped” helplessly within a body whose sensorimotor systems are now controlled by the neuroprosthetic device.<sup>79</sup> Although more sophisticated forms of neural scanning and imaging, computer simulations of the effects of neuroprosthetic devices, research into artificial intelligence, and

---

Robots, and Hybrid Intelligences” (2015); Gladden, “‘Upgrading’ the Human Entity...” (2015).

<sup>79</sup> In a sense, such an occurrence would be the (unfortunate) mirror opposite of those positive situations in which a neuroprosthetic device provides the only means of communication with the outside world for locked-in patients who are completely paralyzed yet fully conscious, including those suffering from ALS, stroke, or traumatic brain injury. For a discussion of such positive cases, see Donchin & Arbel, “P300 Based Brain Computer Interfaces: A Progress Report” (2009).

philosophical thought experiments may be able to provide one with reasonable grounds for suspecting (or doubting) that such a situation is possible, it may be impossible to definitively exclude the possibility if there are no independent means for settling the question outside of the host's own internal conscious experience (or lack thereof).

However remote they might be, such possibilities create particular challenges for risk management, insofar as one must grapple with the risk of an occurrence whose probability of being realized appears incredibly small (but which, in fact, cannot be reliably determined) and whose nightmarish effect on the device's host would, if realized be lethal – if not worse. While philosophers and other researchers have begun to seriously debate such issues (especially with regard to the technological and ontological feasibility of mind uploading<sup>80</sup>), deeper exploration of such issues from ontological, psychological, ethical, legal, and even theological perspectives is required.<sup>81</sup>

### **A growing nexus of information security, medicine, biomedical engineering, neuroscience, and cybernetics**

One aspect of information security highlighted especially by our consideration of advanced neuroprosthetic devices is the growing relationship of information security to fields such as medicine, biomedical engineering, and neuroscience – and the importance that the knowledge developed in these fields will have for shaping the future of information security.<sup>82</sup>

It is already the case that information security is a transdisciplinary field in which personnel must not only be experts in computer hardware and software but must also have knowledge of fields such as psychology, finance, law, and ethics. However, the growing use of neuroprosthetic devices will mean that information security personnel will also need to possess at least basic

---

<sup>80</sup> See Koene, “Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation” (2012); Proudfoot, “Software Immortals: Science or Faith?” (2012); Pearce, “The Biointelligence Explosion” (2012); Hanson, “If uploads come first: The crack of a future dawn” (1994); and Moravec, *Mind Children: The Future of Robot and Human Intelligence* (1990).

<sup>81</sup> For a discussion of many ethical issues relating to neuroprosthetics, see Iles, *Neuroethics: Defining the Issues in Theory, Practice, and Policy* (2006). For an explicit consideration of ethical issues in light of information security concerns (and the possibility that adversaries could potentially wish to gain access to neuroprosthetic devices), see Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009). For theological and spiritual issues relating to neuroprosthetic devices, see Campbell et al., “The Machine in the Body: Ethical and Religious Issues in the Bodily Incorporation of Mechanical Devices” (2008).

<sup>82</sup> For the increasingly inextricable connections between medical devices and information technology, see Gärtner, “Communicating Medical Systems and Networks” (2011).

knowledge about the biological and neuroscientific aspects of such devices. For some large organizations, it may even be desirable and feasible to add to their information security teams physicians, neuroscientists, and biomedical engineers who can work with the other team members to ensure, for example, that any information security mechanisms or practices that the organization implements in relation to its employees' neuroprosthetic devices do not result in biological or psychological harm to the employees. Such medical expertise would also be necessary in order for information security personnel to design safe and effective countermeasures that can be employed against adversaries who possess their own neuroprosthetic devices and attempt to employ them to carry out acts of illicit surveillance or corporate espionage against the company. By employing a knowledge of biology, biomedical engineering, and neuroscience, an organization's information security personnel could develop security controls and countermeasures that neutralize such threats without causing biological or psychological injury to the suspected adversaries for which the company and its information security personnel could potentially be legally and ethically responsible and financially liable.<sup>83</sup>

One challenge that arises in attempting to link information security with medicine is that the two fields utilize different vocabularies and conceptual frameworks: information security is grounded largely in the theoretical framework of computer science while medicine is rooted in that of biology and chemistry. In addressing this challenge, it may be helpful to build on the field of cybernetics, which was founded to provide precisely the sort of transdisciplinary theoretical framework and vocabulary that can be used to translate insights between all of the fields that study patterns of communication and control – whether it be in machines, living organisms such as human beings, or social systems.<sup>84</sup>

Alongside the many existing manifestations of cybernetics (found in subdisciplines such as biocybernetics, neurocybernetics, and management cybernetics) it may be useful to envision a sort of “celyphocybernetics”<sup>85</sup> that sees the human brain, its surrounding body, and any neuroprosthetic devices, implantable computers, and other internal or external technological systems that are integrated into the body as together forming a single physical “shell” for the human mind that possesses that body. The human brain, body, and technological devices together constitute a system that receives information from the external environment, processes, stores, and utilizes information

---

<sup>83</sup> For a related discussion regarding questions about the legality and ethicality of undertaking offensive countermeasures against botnets, see Leder et al., “Proactive Botnet Countermeasures: An Offensive Approach” (2009).

<sup>84</sup> See Wiener, *Cybernetics* (1968).

<sup>85</sup> From the Ancient Greek *κέλυφος*, meaning ‘shell,’ ‘sheath,’ ‘husk,’ or ‘pod.’



circulating within the system, and transmits information to the external environment, thereby creating networks of communication and control. In such a model, information security experts, physicians, and biomedical engineers would thus share the single task of ensuring the secure, productive, and effective functioning of this entire information system that may contain both biological and electronic components – with that common goal only being achievable if all of the expert personnel involved succeed in fulfilling their unique individual roles.

### **The need for new conceptual frameworks: ontologies, typologies, and protocols for information security for neuroprosthetics**

Thanks to decades of tireless visionary labor by researchers and practitioners, there now exists a coherent body of knowledge and best practices relating to information security for computerized information systems that is well-developed and battle-tested and which is being continually refined to deal with new kinds of threats. While those experts who will strive to provide information security for advanced neuroprosthetic devices will be able to ground their efforts in the existing practice of information security for computerized information systems, that general body of knowledge will, on its own, prove to be an inadequate source and guide for their efforts – because advanced neuroprosthetic devices are not simply computerized information systems. In many cases, an advanced neuroprosthetic device simultaneously possesses at least three different natures: it combines in a single device 1) a computerized information system with 2) an implantable medical device and 3) a posthuman technology that has the potential to transform the mind of its human host and radically reshape its user's relationship with his or her own mind and body, with other human beings, with technological systems, and with the external environment as a whole.

Taking into account all of the issues that we have considered earlier in this chapter, it becomes apparent that practices and mechanisms designed to protect the information security of generic computerized information systems are insufficient – if not irrelevant or, in some cases, even counterproductive – when it comes to protecting the information security of advanced neuroprosthetic devices and their device-host systems.<sup>86</sup> As a result, many existing

---

<sup>86</sup> Regarding, e.g., the need for new regulatory frameworks relating to implanted ICT devices, see Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants” (2012). For an example of the complexities involved with determining

neuroprosthetic devices do not incorporate adequate security controls and do not sufficiently protect the privacy of their human hosts and users.<sup>87</sup>

We would argue that in order to implement robust and effective approaches for advancing the information security of advanced neuroprosthetic devices as information systems, medical devices, and transformative posthuman technologies, new conceptual frameworks will first need to be explicitly developed. Such frameworks include **device ontologies** that help one to identify and describe the relevant characteristics of a neuroprosthetic device in a systematic manner; **typologies** that use the ontologies to categorize different neuroprosthetic devices into groups that possess similar relevant characteristics; and neuroprosthetic security **protocols** that define specific device characteristics and operational practices that should be implemented in particular circumstances, based on the needs of a device's host and operator and the broader context of the device's use (including legal, ethical, and organizational considerations). Throughout the remainder of this book we will propose and explore several such frameworks. While they are designed primarily to address the unique circumstances of advanced neuroprosthetic devices, they may also yield insights that can be adapted for promoting the information security of a broader array of future "neurotech" and its human users.

---

which regulations and standards apply to which kinds of medical systems and devices, see Harrison, "IEC80001 and Future Ramifications for Health Systems Not Currently Classed as Medical Devices" (2010). For the inadequacy of traditional information security frameworks as applied to e-healthcare in general, see Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010).

<sup>87</sup> See Tadeusiewicz et al., "Restoring Function: Application Exemplars of Medical ICT Implants" (2012).



## Part II

# **Developing New Conceptual Frameworks**



## Chapter Four

# An Information Security Device Ontology for Advanced Neuroprosthetics

### Introduction to the ontology

In order to create an effective information security framework for neuroprosthetics, it is necessary to first develop an appropriate ontology for such devices. Such an ontology should define the range of possible values for relevant characteristics that are critical for information security and whose values can vary across the universe of neuroprosthetic devices. The ontology should include both the physical characteristics, processes, and contexts and relationships possessed by such devices; it thus differs from (and is necessary for the effective development of) security configuration checklists<sup>1</sup> that would be used to configure particular neuroprosthetic devices for secure operation in their individual human hosts.

Scholars and device manufacturers have made efforts to create general ontologies for robotic systems<sup>2</sup> and mobile devices,<sup>3</sup> however there has not yet been developed an ontology that focuses on the information security characteristics of neuroprosthetic devices. In part, the lack of creation of such formal tools is an effect of the relatively low level of interaction and collaboration between the fields of information security and biomedical engineering.<sup>4</sup>

By synthesizing information gathered from a review of current literature and practice in the fields of neuroprosthetics, implantable computing, and information security, we develop one such ontology within this chapter. Note that because many neuroprosthetic devices are also computers, mobile devices, or implantable medical devices, any generalized information security ontology that is applicable to computers, mobile devices, or IMDs will also

---

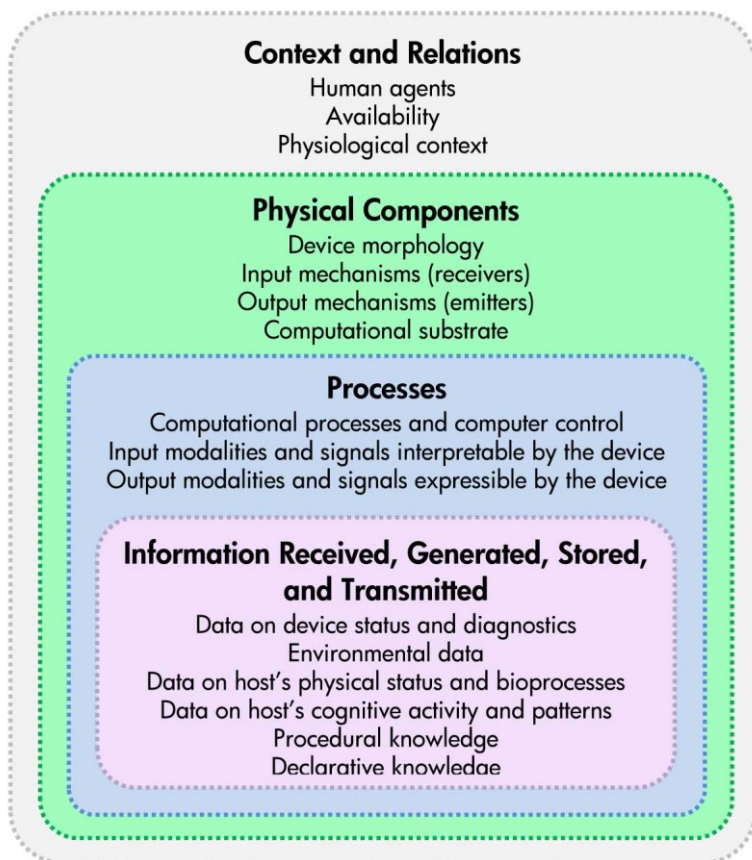
<sup>1</sup> *NIST SP 800-70, Rev. 2* (2011).

<sup>2</sup> See Prestes et al., “Towards a Core Ontology for Robotics and Automation” (2013).

<sup>3</sup> See “FIPA Device Ontology Specification” (2002).

<sup>4</sup> See Clark & Fu, “Recent Results in Computer Security for Medical Devices” (2012).

apply to the relevant kinds of neuroprosthetic devices. The specialized ontology developed here can be understood as a more detailed and focused extension and complement to such ontologies that analyzes the form and functioning of neuroprosthetic devices from the perspective of their particular information security features and risks.



**Figure 1.** The four main areas constituting the information security device ontology for advanced neuroprosthetics, along with the particular variables taken into account within each area.

As is illustrated in Figure 1 above, our ontology is organized into four areas. It categorizes neuroprosthetic devices according to: 1) their context and rela-

tions; 2) their physical components; 3) their processes; and 4) the data, information, and knowledge that is received, stored, and transmitted by the devices.

Each area comprises a number of individual characteristics which we address in detail in the following sections. Together, a device's values for these variables comprise the information security profile for that particular neuroprosthetic device. The ontology presumes that a neuroprosthetic device is an implantable unit, but it can also be applied to nonimplantable external systems (in which case a few of the specific characteristics may not be relevant).

## First area: context and relations

This part of the ontology describes the physical, socioeconomic, and political context in which a neuroprosthetic device is being employed. This context helps determine which individuals have access to the device and for what purposes it may be used. Specific characteristics in this area are:

### Human agents

The human agents<sup>5</sup> who are in different ways responsible for a neuroprosthetic device's functioning include its:

- **Designer**,<sup>6</sup> who determines the basic parameters for the device's form and functioning.
- **Manufacturer**, which physically implements the neuroprosthetic device's design and controls its wholesale distribution<sup>7</sup> and which likely has a unique history of past information security practices, product security flaws, and responses to those flaws.<sup>8</sup>
- **Regulators**,<sup>9</sup> who exercise legal and political power within local, national, or international bodies, who may require or forbid that the device possess certain physical components, processes, or functions, and who may mandate or restrict its distribution and use for certain classes

---

<sup>5</sup> On the impact of such human agents, see Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

<sup>6</sup> Regarding the importance of a device's designer, see Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012), and McCullagh et al., "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology" (2013).

<sup>7</sup> For a device ontology that incorporates manufacturer information, see "FIPA Device Ontology Specification" (2002).

<sup>8</sup> See *NIST SP 800-100* (2006).

<sup>9</sup> On the role of regulators and regulation, see McCullagh et al., "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology" (2013); Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008); and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012).



of users. Multiple jurisdictions may be involved, since a neuroprosthetic device's human host can travel between and within geographically dispersed locations and devices can potentially transmit data to or be controlled from remote locations that are distant from the site at which the device and its user are currently located.

- **Owner**, who owns the physical device but may or may not be the host in whom the device is implanted and may or may not own the rights to intellectual property that is produced by or stored in it. If a device is leased to a user rather than sold, the device's manufacturer or an intermediary firm leasing it to the end user may remain the device's owner.
- **Host** in whose body the neuroprosthetic device has been temporarily or permanently implanted. Depending on the nature of the device, the host may or may not realize that it has been implanted<sup>10</sup> and may or may not have an ability to consciously control or exploit the device's functioning. A host could potentially contribute to or actively undermine the secure functioning of a device.<sup>11</sup>
- **User (or operator)** who has the ability to monitor and consciously control or exploit the device's functioning.<sup>12</sup> In the case of neuroprosthetic devices, the operator might collectively be the medical staff in a hospital who remotely monitor and control the device's operation, rather than the human host in whose body the device has been implanted.<sup>13</sup>

---

<sup>10</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>11</sup> For psychological, social, and cultural factors that might cause the host of an implanted device to intentionally ignore, disable, or otherwise subvert a device's security features and mechanisms – despite the host's awareness that this might put him or her at greater risk of harm – see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010).

<sup>12</sup> See *NIST SP 800-100* (2006) and Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012). For the extent to which the organizational culture and constraints of a device's operator can affect information security, see Cavallari, "Organisational Constraints on Information Systems Security" (2011). For ways in which power relationships between, e.g., the owner, host, and operator of a device might affect compliance with information security policies and procedures that have been developed by one or more of the parties, see Kolkowska & Dhillon, "Organizational Power and Information Security Rule Compliance" (2011).

<sup>13</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012). While the use of remotely controlled implantable devices creates the possibility of illicit surveillance of a device's human host by medical personnel, such remote monitoring may also have positive effects – e.g., making it easier to gather needed medical data from individuals who consider implanted devices less bothersome than external systems; see Lorence et al., "Transac-

A military unit may be the operator of devices implanted in military personnel. A governmental intelligence agency, corporate business intelligence offices, or cybercriminals may be the operators of devices that were implanted (or have been hijacked) for use in surveillance, intelligence-gathering, or espionage.

## Factors impacting availability

Factors determining the extent to which a neuroprosthetic device (and its related external system components, replacement parts, software, and technical manuals) may be available for acquisition by intended or unintended users include its:

- **Licensing and legality**,<sup>14</sup> which may ban certain kinds of neuroprosthetic devices altogether and require medical certification for those implanting other kinds of neuroprosthetics and medical prescriptions for their hosts.
- **Cost**, which may place significant practical limits on the ability of individuals or organizations to acquire neuroprosthetic devices or their components or maintenance equipment.<sup>15</sup>
- **Required expertise**<sup>16</sup> that is needed to acquire, implant, and operate neuroprosthetic devices may significantly limit their potential use.<sup>17</sup>
- **Required maintenance**<sup>18</sup> may restrict use of devices to institutions or individuals that possess appropriate maintenance facilities and supply chains.
- **Required user customization**<sup>19</sup> may limit devices' availability, if a device must be extensively customized for each host or user – whether

---

tion-Neutral Implanted Data Collection Interface as EMR Driver: A Model for Emerging Distributed Medical Technologies" (2009). Implantable devices can allow remote care for those in underserved remote areas and potentially increase efficiency while decreasing cost and aggravations associated with in-hospital care; see Reynolds et al., "Device Therapy for Remote Patient Management" (2008).

<sup>14</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012).

<sup>15</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), and Park et al., "The Future of Neural Interface Technology" (2009).

<sup>16</sup> See Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012), and Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>17</sup> For issues relating to the training of users of BCI systems, see Neuper & Pfurtscheller, "Neurofeedback Training for BCI Control" (2009).

<sup>18</sup> See *NIST SP 800-100* (2006).

<sup>19</sup> See Merkel et al., "Central Neural Prostheses" (2007); Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); and Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008).

through physical fittings of prosthetics, adaptation of device software to a host's unique neurological or behavioral characteristics, or assurance of biological and genetic compatibility (for devices with organic components<sup>20</sup>). Similarly, the ability to use devices may be limited if the anatomical structures, biological processes, or psychological activity of potential hosts or users must be "customized" prior to or after implantation in order to allow operation of the device.

- **Reusability** of a device, which can increase the availability of previously implanted neuroprosthetic devices and require effective procedures for the disposal of devices after use in order to ensure information security.<sup>21</sup>

## Physiological context

The relevant aspects of an implantable neuroprosthetic device's context and situation within its host's body include the:

- **Lifespan** that the device is expected to demonstrate<sup>22</sup> before it requires replacement<sup>23</sup> or invasive maintenance.
- **Physical situation in the body**, which includes the neuroprosthetic device's specific location within the host's body and its physical connections to bodily organs and which also affects the device's:
  - **Physical visibility and discoverability**<sup>24</sup> to both the human host and other human beings interacting with the host.
  - **Physical access to alter the device**,<sup>25</sup> as the fact that a neuroprosthetic device is visibly present does not necessarily entail the possibility of physically accessing the device's key components.
  - **Remote discoverability**, the ability of external devices such as X-ray scanners, millimeter wave scanners, Wi-Fi routers, or Bluetooth

---

<sup>20</sup> See Merkel et al., "Central Neural Prostheses" (2007).

<sup>21</sup> See *NIST SP 800-100* (2006).

<sup>22</sup> See Merkel et al., "Central Neural Prostheses" (2007).

<sup>23</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>24</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

<sup>25</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

devices to identify and localize the neuroprosthetic device from outside of its host's body, even when the device is not visible.<sup>26</sup>

- **Level of neurocognitive interface** between the neuroprosthetic device and the conscious awareness and unconscious cognitive activities of its human host.<sup>27</sup> This includes the extent to which the device's host (who may be different from its primary user) is consciously aware<sup>28</sup> of the device's presence, status, and activity, and the extent to which the device's functioning is determined by the host's neural activity. For example, devices serving as part of an input neural interface system might electrically stimulate afferent neurons to provide sense data to their human host,<sup>29</sup> while mnemoprosthetic devices might interact with interneurons in the host's brain to participate in processes of memory encoding, storage, and retrieval.
- **Health sensitivity and criticality.** A neuroprosthetic device that can directly affect, for example, the functioning of its host's heart or brain requires more safeguards than one that has no such capacity.

## Second area: physical components

This part of the ontology describes the key physical components of the neuroprosthetic device that have implications for information security. Specific characteristics of this area are:

### Device morphology

The device's basic physical morphology includes its:

- **Identity and unitarity**, which describe whether the neuroprosthetic device is a single, clearly identifiable physical unit, or whether the device comprises a large number of small physical components (such as a nanorobot swarm<sup>30</sup>) whose nature and location cannot easily be identified.
- **Size**<sup>31</sup> of the neuroprosthetic device (whether a unit implanted within the host's body or an external unit).

<sup>26</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>27</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); "FIPA Device Ontology Specification" (2002); and Merkel et al., "Central Neural Prostheses" (2007).

<sup>28</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>29</sup> See Park et al., "The Future of Neural Interface Technology" (2009).

<sup>30</sup> See McGee, "Bioelectronics and Implanted Devices" (2008).

<sup>31</sup> See "FIPA Device Ontology Specification" (2002).

- **Materials** from which the device is constructed.<sup>32</sup> While some neuroprosthetic devices may be wholly electromechanical devices, others may include organic (and perhaps even living<sup>33</sup>) components.
- **System participation.**<sup>34</sup> While some neuroprosthetic devices might function as standalone devices, others may simply be the implanted portion of a larger system that also includes monitoring and control equipment outside of the host's body<sup>35</sup> or external actuators or other components (or even entire external systems, such as an exoskeleton, vehicle, or 3D printer) that are remotely controlled by the neuroprosthetic device.<sup>36</sup> Multiple implanted neuroprosthetic devices may also interact to form an implanted body area network (BAN).<sup>37</sup>

### Input mechanisms: physical receivers of matter, energy, and information

A neuroprosthetic device's physical mechanisms for receiving input in the form of matter, energy, or information<sup>38</sup> may include:

- **A power supply.**<sup>39</sup> Important are both the nature of the device's primary power source (whether an internal battery, external wireless or wired power supply, or power supplied by the host's organism), the ability to utilize any backup or alternative power sources, and the behavior that the device will demonstrate if its primary (or only) supply of power is lost.
- **Physical ports and controls** such as on/off switches, microSD card slots, or micro-USB or proprietary communication ports.<sup>40</sup>

---

<sup>32</sup> See McGee, "Bioelectronics and Implanted Devices" (2008).

<sup>33</sup> See Merkel et al., "Central Neural Prostheses" (2007).

<sup>34</sup> See Prestes et al., "Towards a Core Ontology for Robotics and Automation" (2013), and *NIST SP 800-100* (2006).

<sup>35</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), and Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009).

<sup>36</sup> See Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

<sup>37</sup> See Sayrafian-Pour et al., "Channel Models for Medical Implant Communication" (2010).

<sup>38</sup> See "FIPA Device Ontology Specification" (2002).

<sup>39</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Merkel et al., "Central Neural Prostheses" (2007); and Li et al., "Advances and Challenges in Body Area Network" (2011).

<sup>40</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

- **Environmental sensors** through which the neuroprosthetic device receives input from the environment outside of its host's body. This may include:
  - **Specialized data reception mechanisms**<sup>41</sup> such as photoreceptors, ultrasonic sensors,<sup>42</sup> or radio receivers that are intentionally designed to detect particular signals for processing by the device.
  - **Unpurposeful receptors** in the form of components that were not designed to function as sensors but which can nevertheless be affected by environmental phenomena (such as electromagnetic radiation, heat, or acceleration). Many, if not all, of a device's components will be unpurposeful receptors (in addition to whatever other roles they might fill), insofar as their structure or performance can be affected by external forces or phenomena.
- **Neuronal input mechanisms**<sup>43</sup> through which the device receives electrochemical signals from either afferent neurons, efferent neurons, or interneurons within the host's body, potentially through a brain-computer interface (BCI).<sup>44</sup> Input can come from a large group of neurons or a single neuron.<sup>45</sup>

## Output mechanisms: physical emitters of matter, energy, and information

The device's physical mechanisms for generating output in the form of matter, energy, or information may include:<sup>46</sup>

---

<sup>41</sup> See "FIPA Device Ontology Specification" (2002); Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Park et al., "The Future of Neural Interface Technology" (2009); Merkel et al., "Central Neural Prostheses" (2007); and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>42</sup> See Warwick & Gasson, "Implantable Computing" (2008).

<sup>43</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010), and Park et al., "The Future of Neural Interface Technology" (2009).

<sup>44</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Merkel et al., "Central Neural Prostheses" (2007).

<sup>45</sup> Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010), and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>46</sup> See "FIPA Device Ontology Specification" (2002), pp. 6-8, for an example of how such mechanisms could be described and categorized

- **Physical actuators** such as robotic prostheses that are controlled by the neuroprosthetic device.<sup>47</sup> Speakers used to broadcast synthesized speech<sup>48</sup> are also, in a sense, highly specialized actuators.
- **Environmental emitters** through which the neuroprosthetic device affects the environment outside of its host's body.<sup>49</sup> This may include:
  - **Specialized data transmission mechanisms**<sup>50</sup> such as radio,<sup>51</sup> optical, and ultrasonic transmitters and electromagnetic induction mechanisms that have been intentionally designed.<sup>52</sup>
  - **Unpurposeful emitters** in the form of components that were not designed to function as transmitters but which can nevertheless affect the external environment (e.g., by producing audible sounds or electromagnetic radiation).
- **Neuronal output mechanisms**<sup>53</sup> through which the device transmits electrochemical signals to either afferent neurons, efferent neurons, or interneurons within the host's body, potentially through a BCI.<sup>54</sup>

## Computational substrate

In their role as computers, some neuroprosthetic devices may display a physical computational architecture based on the execution of programs by a serial processor; others may take the form of a physical neural network that

---

<sup>47</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); Merkel et al., "Central Neural Prostheses" (2007); Lebedev, "Brain-Machine Interfaces: An Overview" (2014); and Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

<sup>48</sup> See Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008).

<sup>49</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>50</sup> See "FIPA Device Ontology Specification" (2002) and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>51</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>52</sup> Regarding the importance of reliable data-transport systems for transmitting data from an implanted device to other implanted devices or external systems, see Fernandez-Lopez et al., "The Need for Standardized Tests to Evaluate the Reliability of Data Transport in Wireless Medical Systems" (2012).

<sup>53</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); and Park et al., "The Future of Neural Interface Technology" (2009).

<sup>54</sup> See Merkel et al., "Central Neural Prostheses" (2007).

does not execute programs. An information security ontology should describe the specifications of a device's:

- **CPU-based systems**<sup>55</sup> (if applicable) which can be used to execute traditional software programs. These processing abilities are constrained by the characteristics of a system's:
  - **Processor(s)**, which might take the form of a single central processing unit (CPU),<sup>56</sup> a multicore computer, or a CPU-based cluster or grid.
  - **Memory**,<sup>57</sup> which might include volatile RAM used as primary storage, non-volatile RAM used as longer-term secondary storage, and non-volatile ROM used for storing firmware or data that should not be altered.
- **Physical neural networks** (if applicable) that comprise a large number of artificial neurons that transmit signals to one another through artificial synapses and which store data in the form of activation patterns within the networks. While capable of processing input, making decisions, generating output, and learning, such networks do not execute traditional computer programs. A physical neural network's capacities are determined by the type, specifications, and quantity of neurons that constitute the network.

### Third area: processes

This part of the ontology describes the key computational or cognitive processes carried out by the neuroprosthetic device that have implications for information security. Specific characteristics of this area are:

#### Computational processes and computer control

While a neuroprosthetic device can potentially operate with full autonomy (or may be subject to control by the unconscious biological processes of its human host at a biochemical level, in the case of passive neuroprosthetic devices), such devices typically incorporate some means by which their users can exercise at least partial control over a device after its implantation. However, even a device that is ultimately controlled by a human user often still carries out some internal procedures for processing data in order to make

---

<sup>55</sup> See "FIPA Device Ontology Specification" (2002).

<sup>56</sup> See "FIPA Device Ontology Specification" (2002).

<sup>57</sup> See "FIPA Device Ontology Specification" (2002), and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).



decisions and generate actions.<sup>58</sup> The kinds of computational processes available to a neuroprosthetic device will depend on the kind of physical substrate upon which the processes are performed. The ontology includes specifications for a device's:

- **Level of autonomy.** As is the case for robotic systems, a neuroprosthetic device might function autonomously, semi-autonomously, or as a telepresence device under the full and direct control of its operator.<sup>59</sup> The level of autonomy is related to a neuroprosthetic device's:
  - **Capacity for control by its human host,**<sup>60</sup> as a device might be designed to respond to instructions delivered by its host via means such as oral verbal commands, instructions typed into a keypad or into the device's housing, or electrochemical signals from individual neurons or groups of neurons.<sup>61</sup>
  - **Capacity for control via teleoperation,** which may allow a neuroprosthetic device to be remotely controlled by external devices or by a user other than its human host.<sup>62</sup>
- **Computer programs** that can be run by a neuroprosthetic device utilizing a CPU-based system. The specifications for such a device should describe its:
  - **Operating system,**<sup>63</sup> which may be designed or installed by the device's manufacturer and include certain built-in diagnostic programs.
  - **Applications**<sup>64</sup> that can be stored and executed by the device to expand its functionality and which may be produced by its manufacturer, user, host, or third-party software developers.

---

<sup>58</sup> See Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>59</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>60</sup> See "FIPA Device Ontology Specification" (2002) for information about user controls.

<sup>61</sup> See Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

<sup>62</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>63</sup> See "FIPA Device Ontology Specification" (2002) and Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

<sup>64</sup> See Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

- **Software update methods** that allow the device's operating system and applications to be modified after the device has been implanted in its human host.<sup>65</sup>
- **Neural computing** (if applicable). Here we use “neural computing” to describe the manner in which a neural network assimilates input and utilizes the information contained in its activation patterns to generate decisions and actions; this represents a means of computation different from the execution of traditional computer programs. A device that utilizes a physical neural network will thereby instantiate a neural computing process.<sup>66</sup> Some CPU-based systems may execute software that simulates a neural network,<sup>67</sup> however at their most fundamental level, such systems' computational processes are computer programs, not neural computing processes as defined here. At a minimum, the specifications of a neural computing process will describe: a) *the patterns of connection* between neurons; b) *the means by which connection weights are updated* (i.e., the learning mechanism); and 3) *the activation function* by which an individual neuron converts input to output.

### Input modalities and signals interpretable by the device

A neuroprosthetic device is typically capable of processing and interpreting certain kinds of signals received through its input mechanisms to extract or synthesize information (or perhaps even knowledge) that can potentially be compressed, stored, transmitted, transformed, and used to inform or control the device's operation.<sup>68</sup> A neuroprosthetic device may be able to recognize and extract meaning from input that arrives in the form of:

- **Machine communication protocols** such as TCP/IP, Bluetooth, 3G, and proprietary NFC formats.<sup>69</sup>
- **Environmental signals.** If a neuroprosthetic device possesses sufficiently advanced AI, it might be able to extract meaning directly from sensory input that it receives from the environment outside its host's

---

<sup>65</sup> See Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012), and McGee, “Bioelectronics and Implanted Devices” (2008).

<sup>66</sup> For an excellent discussion of the distinction between a physical neural network and the neural computational processes that may be occurring within it, see Mizraji et al., “Dynamic Searching in the Brain” (2009).

<sup>67</sup> See Merkel et al., “Central Neural Prostheses” (2007), and Lebedev, “Brain-Machine Interfaces: An Overview” (2014).

<sup>68</sup> See Merkel et al., “Central Neural Prostheses” (2007).

<sup>69</sup> See “FIPA Device Ontology Specification” (2002); Li et al., “Advances and Challenges in Body Area Network” (2011); and Tarin et al., “Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring” (2009).

body. It may convert raw sensory data into modalities analogous to those that are accessible to human beings (such as identifiable sights, sounds, touches, tastes, smells, and proprioception that fall within the human range of perception).<sup>70</sup>

- **Natural human communication** which might be provided by the device's human host or user in the form of: a) *textual verbal input*<sup>71</sup> such as typed or emailed instructions that can be interpreted through an application of artificial intelligence; b) *oral verbal input*<sup>72</sup> such as spoken natural-language instructions that are identified through speech recognition software; and c) *nonverbal input*<sup>73</sup> such as gestures, eye gaze, or vocal intonation on the part of its human host or external user.
- **The host's biological processes**<sup>74</sup> which contain data such as those reflected in brain activity,<sup>75</sup> cardiac rhythms, and blood chemistry that can be interpreted by a neuroprosthetic device in a way that that recognizes particular patterns within the data that trigger some predetermined response. The patterns found in such data may or may not be under the conscious control of the device's host, depending on whether the data comprise: a) *the host's cognitive activity and patterns*,<sup>76</sup> which may include emotional states,<sup>77</sup> memories, volitions,<sup>78</sup> and sensory percepts; or b) *the host's motor activity and actions*, as even without direct access to the host's cognitive activity, a device might use techniques such as electromyography to detect and interpret electrical activity indicating voluntary contraction of a host's muscles.<sup>79</sup>

---

<sup>70</sup> See Merkel et al., "Central Neural Prostheses" (2007), and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>71</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>72</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

<sup>73</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010), and Rao & Nayak, *The InfoSec Handbook* (2014).

<sup>74</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>75</sup> See Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

<sup>76</sup> See McGee, "Bioelectronics and Implanted Devices" (2008).

<sup>77</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>78</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>79</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement"

Note that while a neuroprosthetic device might be able to receive and store many other kinds of input, only those forms of input whose modalities are interpretable by the device will typically have the potential to trigger purposeful and targeted responses by the device's computational processes.

## Output modalities and signals expressible by the device

In its capacity as an implantable computer, a neuroprosthetic device is typically capable of generating output in forms that can be interpreted by a human being or external device and which may carry specific meanings and may be used to influence or control the behavior of external entities in purposeful ways.<sup>80</sup> A device may be able to generate such output transmitted via:

- **Machine communication protocols** such as TCP/IP, Bluetooth, 3G, and proprietary NFC formats.<sup>81</sup>
- **Environmental signals.** If a neuroprosthetic device possesses sufficiently advanced computational processes, it might be able to directly encode messages in the form of physical output released into the environment external to its host's body or perhaps transmitted to its host through physical displays<sup>82</sup> or virtual reality equipment in the form of sensory modalities directly accessible to human beings (such as identifiable sights, sounds, touches, tastes, smells, and proprioception that fall within the human range of perception).
- **Natural human communication** which might take the form of: a) *textual verbal output*<sup>83</sup> provided to the device's host (e.g., either as messages appearing on a physical display screen on the device's visible housing or as messages overlaid in the host's field of vision, either through the use of an external virtual reality display or through the direct transmission of signals to the host's retinal ganglion cells, optic nerve, or interneurons in the brain) or to an external user (e.g., as messages displayed on an external accessory device or sent as ordinary emails); b) *oral verbal output*,<sup>84</sup> which might take the form of synthesized speech that is broadcast aloud through an external physical

---

(2012), and Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>80</sup> See Merkel et al., "Central Neural Prostheses" (2007).

<sup>81</sup> See "FIPA Device Ontology Specification" (2002); Li et al., "Advances and Challenges in Body Area Network" (2011); and Tarin et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009).

<sup>82</sup> See "FIPA Device Ontology Specification" (2002).

<sup>83</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

<sup>84</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

speaker, that is “heard” by participants within some virtual reality environment, that is heard by the device’s host through the direct transmission of signals to the host’s cochlear nerve or to interneurons in the brain, or that might be generated by the host’s own vocal cords, if the device is able to directly stimulate them; or c) *nonverbal output* such as gestures, eye gaze, or tone of voice, which could be displayed either by means of the device’s control over its host’s natural body, through the device’s control of prosthetic components in the host’s body, or through the device’s manifestation as a digital avatar with a physical appearance within a virtual reality environment.

- **Host’s biological processes** that can potentially be influenced or controlled by the device to produce particular phenomena such as brain activity, cardiac rhythms,<sup>85</sup> or changes in blood chemistry<sup>86</sup> that can be noticed and interpreted by the device’s human host. Such patterns might be generated within: a) *the host’s cognitive activity and patterns*, which may include the generation or alteration in the human host of emotional states, memories, volitions, and sensory percepts;<sup>87</sup> b) *the host’s motor activity*,<sup>88</sup> through action of the device upon the host’s efferent neurons or directly upon muscles; or c) *the control of other organs of the host*, by which the device influences or controls the functioning of other organs and systems within the host’s body, either through direct electrochemical stimulation or through the manipulation of other systems within the host’s body to trigger particular responses by organs.

Note that messages and information that a neuroprosthetic device transmits using these modalities may not have been generated by the device itself; e.g., they may have been stored in the device by its user in advance for later transmission, or they could be received live through some sensor and then immediately retransmitted by the device. It is also possible for such information to comprise an underlying stream of “real” sensory data from the external world that has been altered or augmented in some way, or it may be

---

<sup>85</sup> See Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012).

<sup>86</sup> See McGee, “Bioelectronics and Implanted Devices” (2008).

<sup>87</sup> See Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012); McGee, “Bioelectronics and Implanted Devices” (2008); and Patil & Turner, “The Development of Brain-Machine Interface Neuroprosthetic Devices” (2008).

<sup>88</sup> See Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012); McGee, “Bioelectronics and Implanted Devices” (2008); and Fairclough, “Physiological Computing: Interfacing with the Human Nervous System” (2010).

wholly fabricated within the neuroprosthetic device (or on an external device that transmits it to the neuroprosthetic device), to create a virtual reality environment to be experienced by the neuroprosthetic device's host. Such capacities could potentially be used in harmful (or at least manipulative) ways<sup>89</sup> if the device's functioning has been compromised by a virus or hacked by an unauthorized user.

## Fourth area: data, information, and knowledge received, generated, stored, and transmitted

The information security profile of an implantable neuroprosthetic device is shaped not only by the processes through which the device manipulates information or the physical locations in which the information is stored but also by the kinds of information involved.<sup>90</sup> Note that a neuroprosthetic device may be able to receive, generate, store, and transmit<sup>91</sup> types of information that the device itself cannot directly interpret or utilize (e.g., encrypted files that have been saved to the device by its user). This part of the ontology specifies the device's reception, storage, and transmission of:

### Data regarding the device's status and diagnostics

A neuroprosthetic device may handle information about its own internal status and functioning, which may be: a) *receivable by the device*, either from components internal to the device or from external monitors; b) *generated by the device*; c) *stored on the device* (e.g., in the form of logfiles); and d) *transmitted by the device* (e.g., to remote external components of the neuroprosthetic system or to medical personnel who are monitoring the device's status to ensure proper functioning).

### Environmental data

An implantable neuroprosthetic device may handle data about the environment exterior to its host's body similar to those gathered by human sensory organs.<sup>92</sup> Such information may be: a) *receivable by the device* through its own sensors or from afferent neurons in the host's body; b) *generated by the device*; c) *stored on the device* before or after undergoing processing; and d) *transmitted by the device* (e.g., to its human host as though it were sense data obtained directly by the host's own sensory organs, or to external systems or individuals who might use the data in teleoperation of the device).

---

<sup>89</sup> Regarding possibilities of neuroprosthetics being used to provide false data or information to their hosts or users, see McGee, "Bioelectronics and Implanted Devices" (2008), p. 221.

<sup>90</sup> See Rao & Nayak, *The InfoSec Handbook* (2014).

<sup>91</sup> See Li et al., "Advances and Challenges in Body Area Network" (2011).

<sup>92</sup> See McGee, "Bioelectronics and Implanted Devices" (2008).

## Data regarding the host's physical status and biological processes

A neuroprosthetic device may handle highly sensitive information about the identity, location, health, and biological processes of its human host.<sup>93</sup> Such information may be: a) *receivable by the device* (e.g., through sensors directly monitoring the host's biological processes<sup>94</sup>); b) *generated by the device*; c) *stored on the device* after being gathered and processed by the device;<sup>95</sup> and d) *transmitted by the device* (e.g., through wireless communication to medical personnel who are remotely monitoring the host's medical condition and controlling the device to administer telemedicine services<sup>96</sup>).

## Data regarding the host's cognitive activity and patterns

In addition to information about more general biological processes, an implantable neuroprosthetic device with the appropriate form of neural connectivity could potentially receive, generate, store, and transmit – in at least limited fashion – information about the contents of its host's cognitive processes,<sup>97</sup> including emotional states, memories,<sup>98</sup> and volitions.<sup>99</sup> Such information might be: a) *receivable by the device* (e.g., through a BCI that can remotely detect activity in the host's brain or which interacts directly with interneurons in the brain through artificial synapses); b) *generated by the device* (e.g., through its analysis of other data); c) *stored on the device* for later processing and analysis, even if the device itself is incapable of performing such

---

<sup>93</sup> See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010), and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012).

<sup>94</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>95</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>96</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>97</sup> See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009); and Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

<sup>98</sup> For the possibility of developing mnemoprosthetics, see Han et al., "Selective Erasure of a Fear Memory" (2009), and Ramírez et al., "Creating a False Memory in the Hippocampus" (2013).

<sup>99</sup> See McGee, "Bioelectronics and Implanted Devices" (2008).

analysis; and d) *transmitted by the device*<sup>100</sup> (e.g., to external medical systems for purposes of analyzing the user's neurological condition or to remote systems where the neural activity can be used to control prosthetic limbs or other robotic devices).

## Procedural knowledge

Procedural knowledge is the body of information needed to perform particular tasks; in the context of a neuroprosthetic device such knowledge might be: a) *receivable by the device* (e.g., in the form of downloadable packages that provide a device with instructions – perhaps including linguistic, social, and cultural information – on how to interact with its human host or user in particular situations); b) *generated by the device*; c) *stored on the device* (e.g., in the form of software<sup>101</sup> that guides the device's routine functioning and specifies how it should carry out particular actions in response to unique events or circumstances); and d) *transmitted by the device* (e.g., in the form of device drivers or other files sent to external devices to allow them to connect with the device and utilize its resources).

## Declarative knowledge

A neuroprosthetic device may handle descriptive or declarative knowledge in a format that is readily comprehensible to (and may have been prepared by) human beings.<sup>102</sup> This might include information contained in everyday correspondence like emails or text messages or the contents of documents downloaded from the Internet. Such information may be: a) *receivable by the device* (e.g., through electronic messages composed by the device's user, downloaded from websites through wireless Internet connections, or recorded in the form oral conversations that undergo speech-to-text processing); b) *generated by the device*; c) *stored on the device* (e.g., as ordinary text files); and d) *transmitted by the device* (e.g., in the form of messages or alerts sent to the device's human host or content downloaded from websites and available on demand for transmission to the host's sensory system for the host to experience).

---

<sup>100</sup> See Tarín et al., “Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring” (2009).

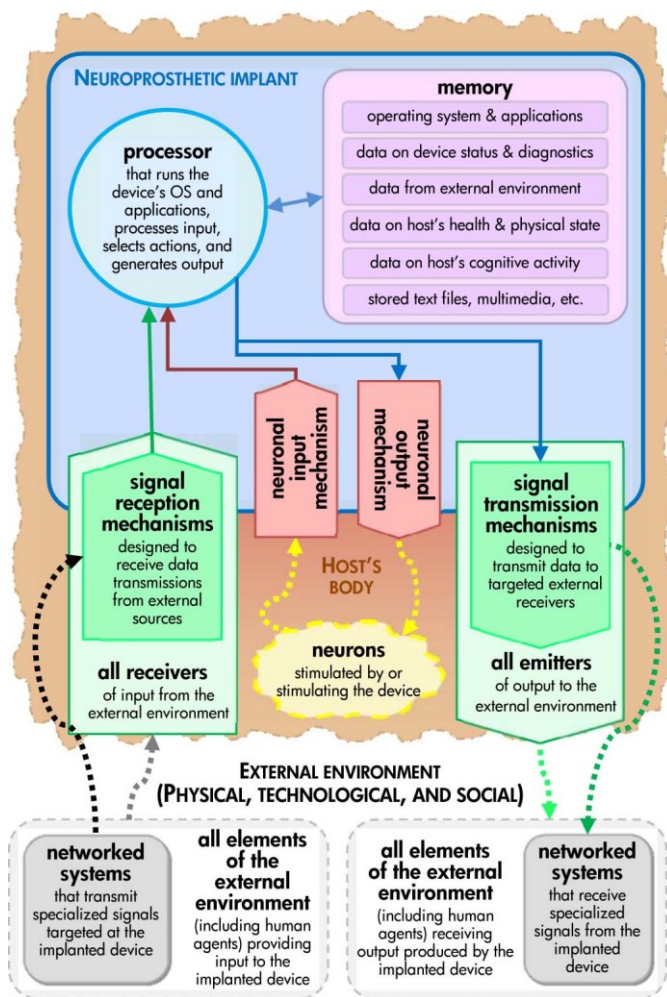
<sup>101</sup> See “FIPA Device Ontology Specification” (2002).

<sup>102</sup> See McGee, “Bioelectronics and Implanted Devices” (2008).



## Toward developing a comprehensive information security framework

In Figure 2 below we can see a sample representation of how the various parts of the ontology are instantiated and interrelate with one another in the case of a particular hypothetical implantable neuroprosthetic device.



**Figure 2.** One possible implementation of an implantable neuroprosthetic device, reflecting a unique profile of characteristics that can be captured and described by the device ontology for information security presented in this chapter.

One can use this ontology to prepare an information security profile for a particular device by working through the ontology step-by-step and specifying the particular characteristics that the device (and its broader support system) possesses or demonstrates for each of the items. Once one possesses a completed ontology for a particular neuroprosthetic device – and thus understands its basic technical specifications and operational context – one can then apply the two-dimensional information security framework developed in the following chapter to understand the impacts that the device will have on its human host and the device’s implications for the information security of its device-host system.



## Chapter Five

# A Two-dimensional Framework of Cognitive Security for Advanced Neuroprosthetics

### Developing a two-dimensional cognitive security framework

In this chapter we develop a two-dimensional conceptual framework for cognitive security. The first dimension includes nine essential information security attributes or goals for neuroprosthetic devices and device-host systems, namely **confidentiality**, **integrity**, **availability**, **possession**, **authenticity**, **utility**, **distinguishability**, **rejectability**, and **autonomy**. Each of these attributes relates to the device-host system as understood at three different levels, which comprise the second dimension of the framework; the levels are those of the device's host understood as **sapient metavolitional agent**, **embodied embedded organism**, and **social and economic actor**. Below we present this framework in detail and consider its implications for information security for advanced neuroprosthetic devices.

### Defining security goals for the entire device-host system: nine essential attributes

One of the most fundamental ways of understanding information security is through a framework of essential characteristics that a system must possess in order to be secure. One can understand these characteristics as the security “attributes” that an ideal system would possess. However, in practice such characteristics can never be perfectly achieved, and thus rather than envisioning them as a system's optimal state, they can instead be understood as the security “goals” that one is perpetually striving to attain through the process of information security.

Denning et al. propose a model of “neurosecurity” for neuroprosthetic devices that strives for “the protection of the confidentiality, integrity, and availability of neural devices from malicious parties with the goal of preserving the

safety of a person's neural mechanisms, neural computation, and free will.”<sup>1</sup> While that model provides an excellent starting point (especially with regard to contemporary types of neuroprosthetic devices that are already in use), in itself it is not sufficiently specific or robust to drive the development of mature and highly effective information security plans, mechanisms, and practices that will be capable of protecting neuroprosthetic devices and device-host systems from the full range of threat sources, including expertly skilled and intensely motivated adversaries. In particular, a strong and more comprehensive information security framework will be needed to protect the kinds of highly sophisticated (and even posthuman) neuroprosthetic devices and device-host systems that are expected to become a reality within the coming years and decades.

The cognitional security framework that we develop here for a device-host system utilizing advanced neuroprosthetics includes nine security goals or attributes: three are the elements of the classic CIA Triad (confidentiality, integrity, and availability);<sup>2</sup> three are additional characteristics developed by Donn Parker in his security hexad (possession, authenticity, and utility);<sup>3</sup> and three are new characteristics which we have identified as being uniquely relevant for the security of advanced neuroprosthetics (distinguishability, rejectability, and autonomy).<sup>4</sup> Below we briefly define each of these security goals, with particular reference to their relevance for advanced neuroprosthetics.

## Confidentiality

In the context of an advanced neuroprosthetic system, we can define confidentiality as **“limiting the disclosure of information to only those sapient agents that are authorized to access it.”**

Note that according to this understanding, confidentiality has only been breached if the information is accessed by another “sapient agent” (such as a human being) who is not authorized to do so. For example, imagine that a neural implant is able to detect and record the contents of my thoughts and

---

<sup>1</sup> See Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

<sup>2</sup> Rao & Nayak, *The InfoSec Handbook* (2014), pp. 49-53.

<sup>3</sup> See Parker, “Toward a New Framework for Information Security” (2002), and Parker, “Our Excessively Simplistic Information Security Model and How to Fix It” (2010).

<sup>4</sup> There is ongoing debate about the number and relationship of information security goals and attributes. Other attributes identified by some, such as “completeness” and “non-repudiation/accuracy” (see Dardick’s analysis of IQ, CFA, and 5 Pillars in Dardick, “Cyber Forensics Assurance” (2010)) or “accountability” and “assurance” (*NIST SP 800-33* (2001), p. 3) are not explicitly considered here as independent objectives.

– without my knowledge – is wirelessly transmitting a record of this data to create a “backup copy” of my thoughts on an external computer. While this means that I no longer have sole control or “possession” of the information (as defined below), the creation of such an unauthorized external backup of my thoughts does not in itself represent a loss of confidentiality, as long as the information stored on the external computer is not viewed by some unauthorized person. Confidentiality applies not only to the data stored within a system but also to information about the system itself,<sup>5</sup> insofar as knowledge about a system’s design, functioning, and vulnerabilities makes it easier for unauthorized parties to plan an attack on the system.

Our definition of confidentiality in relation to neuroprosthetics builds on existing definitions of confidentiality used in the field of information security. For example, confidentiality has previously been defined as “the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.”<sup>6</sup> Parker defines confidentiality as the “Limited observation and disclosure of knowledge.”<sup>7</sup> Alternatively, it can be understood as “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.”<sup>8</sup> Glenn Dardick proposes a model of Cyber Forensics Assurance (CFA) in which confidentiality is understood as “ensuring that information is accessible only to those authorized to have access.”<sup>9</sup>

While ensuring that information is not disclosed to unauthorized parties is typically an important organizational goal, preventing the destruction or corruption of the information is often an even more important objective. Thus *NIST SP 800-33* notes that “For many organizations, confidentiality is frequently behind availability and integrity in terms of importance. Yet for some systems and for specific types of data in most systems (e.g., authenticators), confidentiality is extremely important.”<sup>10</sup> As is true for implantable medical devices generally, neuroprosthetic devices constitute a class of systems whose data is often highly sensitive and for which confidentiality is thus a great concern.

---

<sup>5</sup> *NIST SP 800-33* (2001), p. 2.

<sup>6</sup> *NIST SP 800-33* (2001), p. 2.

<sup>7</sup> Parker, “Toward a New Framework for Information Security” (2002), p. 125.

<sup>8</sup> 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37*, Rev. 1 (2010), p. B-2.

<sup>9</sup> Dardick, “Cyber Forensics Assurance” (2010), p. 61. Dardick developed his CFA model by analyzing and synthesizing definitions developed in frameworks such as the CIA Triad as defined in the Federal Information Security Management Act of 2002 (FISMA), the Five Pillars of Information Assurance model developed by the US Department of Defense, the Parkerian Hexad, and the Dimensions of Information Quality developed by Fox and Miller.

<sup>10</sup> *NIST SP 800-33* (2001), p. 2.

## Integrity

With regard to an advanced neuroprosthetic system, we can define integrity as “**remaining intact, free from the introduction of substantial inaccuracies, and unchanged by unauthorized manipulation.**”

As is true for confidentiality, integrity is needed for both the data stored within a system as well as for the storage system itself.<sup>11</sup> The integrity of information in advanced neuroprosthetic systems is a complex issue, especially in the case of neuroprosthetics that are involved with the mind’s processes of forming, storing, and recalling long-term memories. The long-term memories that are stored within our brain’s natural memory systems already undergo natural processes of compression and degradation over time;<sup>12</sup> none of our long-term memories presents a perfect replica of the original experience that led to formation of the memory. While our memories may, over time, lose detail and become more impressionistic, they do not lose “integrity” unless the memory has been transformed in such a way that the meaning that it *does* convey is no longer accurate or no longer presents a coherent whole. According to our definition, a memory also does not lose integrity simply as a result of undergoing manipulation, as long as it is a form of *authorized* manipulation that does not introduce substantial inaccuracies. (Thus a neuroprosthetic device that uses some algorithm to compress memories by identifying and preserving essential details while eliminating inessential elements would not necessarily be damaging the integrity of those memories.)

Within more generalized existing frameworks for information security, data integrity has been defined as “the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit,” and system integrity has been defined as “the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation.”<sup>13</sup> It is alternatively understood as “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.”<sup>14</sup> Parker defines integrity as the “Completeness, wholeness, and readability of information” and the fact that the information remains “unchanged from a previous state.”<sup>15</sup> Dardick’s synthetic CFA model summarizes the joint concept of “Integrity/Consistency” as the “perceived consistency of actions, values, methods,

---

<sup>11</sup> NIST SP 800-33 (2001), p. 2.

<sup>12</sup> See Dudai, “The Neurobiology of Consolidations, Or, How Stable Is the Engram?” (2004).

<sup>13</sup> NIST SP 800-33 (2001), p. 2.

<sup>14</sup> 44 U.S.C., Sec. 3542, cited in NIST SP 800-37 (2010), Rev. 1, p. B-6.

<sup>15</sup> Parker, “Toward a New Framework for Information Security” (2002), p. 125.

measures and principle – unchanged ‘is it true all of the time?’ (Verification).<sup>16</sup> *NIST SP 800-33* suggests that “Integrity is commonly an organization’s most important security objective after availability.”<sup>17</sup>

## Availability

In the context of an advanced neuroprosthetic system, we can define availability as **“the ability to access and experience desired information in a timely and reliable manner.”**

This definition of availability differs somewhat from definitions traditionally used in information security. First, it emphasizes that for the user of a neuroprosthetic system, it is not sufficient for information to be stored in a database from which the user can export or save files with particular subsets of information; it is typically important that the user be able to directly *experience* the information as an object of his or her conscious awareness (e.g., sense data that are presented to one’s mind to be perceived in the form of percepts or memories that can be recalled and thus “re-experienced” in one’s mind at will). Second, this definition emphasizes that it is not sufficient for a user to have access to a vast pool of information, within which the one or two pieces of information that the user would actually like to consciously recall are lost amidst countless streams of information, most of which are at the moment irrelevant to the user’s desires. The users of a neuroprosthetic device must be able to quickly and reliably experience in their conscious awareness the particular piece of information that they desire. In the case of some neuroprosthetics, such as an artificial eye that is conveying sense data from the environment, “quickly” experiencing information effectively means that it must be presented in real time.

Ensuring the availability of information involves maintaining both data and the system or systems that contain it and provide it to users. More generalized frameworks for information security have defined availability as the assurance “that systems work promptly and service is not denied to authorized users;” it involves preventing any “unauthorized deletion of data” or other “denial of service or data” that are either inadvertent or intentional in nature.<sup>18</sup> Availability has alternatively been understood as “Ensuring timely and reliable access to and use of information.”<sup>19</sup> Parker defines availability simply as the “Usability of information for a purpose.”<sup>20</sup> Dardick’s synthetic CFA model understands the joint concept of “Availability/Timeliness” as the

<sup>16</sup> Dardick, “Cyber Forensics Assurance” (2010), p. 61.

<sup>17</sup> *NIST SP 800-33* (2001), p. 2.

<sup>18</sup> *NIST SP 800-33* (2001), p. 2.

<sup>19</sup> 44 U.S.C., Sec. 3542, cited in *NIST SP 800-37* (2010), Rev. 1, p. B-2.

<sup>20</sup> Parker, “Toward a New Framework for Information Security” (2002), p. 124.



“the degree to which the facts and analysis are available and relevant (valid and verifiable at a specific time).”<sup>21</sup>

*NIST SP 800-33* reports that “Availability is frequently an organization’s foremost security objective.”<sup>22</sup> Placing such a high priority on availability is reasonable, for example, in the case of an advanced neuroprosthetic device that provides its user with real-time sense data or support in cognitive processes such as memory or volition, where the loss of availability of the device and its data at a critical moment could result in injury or death.

The goals of confidentiality, integrity, and availability display a number of mutual interdependencies; for example, if a system’s integrity has been lost, its mechanisms for maintaining the confidentiality and availability of its data may no longer be functional or reliable.<sup>23</sup> Some definitions of availability combine two or more different goals by stating that the objective is not only to ensure that data is always available to legitimate users for legitimate purposes but also to ensure that it is always *unavailable* to any person or process that is attempting to use the data (or the larger system) for “unauthorized purposes.”<sup>24</sup> In the framework presented here for neuroprosthetic devices, ensuring availability does not involve preventing information from being accessed by unauthorized parties or authorized parties who would attempt to use the information for unauthorized purposes; instead, security goals such as maintaining the *possession* and *confidentiality* of information represent those objectives.

## Possession

With regard to an advanced neuroprosthetic system, we can define possession as **“holding and controlling the physical substrate or substrates in which information is embodied.”**

This definition requires that in order to have possession of information, the user of a neuroprosthetic device must have *sole* possession. If two different parties own physical copies of some information, then it can be said that the information is *available* to both parties but that neither “possesses” it, insofar as neither party, acting individually, has the ability to prevent the creation of additional physical copies of the information or the distribution of such copies to additional parties.

---

<sup>21</sup> Dardick, “Cyber Forensics Assurance” (2010), p. 61.

<sup>22</sup> *NIST SP 800-33* (2001), p. 2.

<sup>23</sup> *NIST SP 800-33* (2001), p. 4.

<sup>24</sup> *NIST SP 800-33* (2001), p. 2.

Within the framework of the classic CIA Triad, possession is not explicitly defined as a freestanding security goal, however it can be understood implicitly as an aspect of confidentiality and, in some cases, a prerequisite for maintaining integrity and availability. Possession is explicitly delineated as an independent security goal in the expanded Parkerian Hexad, where it is defined as “Holding, controlling, and having the ability to use information.”<sup>25</sup> Meanwhile, Dardick’s synthetic CFA model summarizes the joint concept of “Possession/Control” as relating to the “chain of custody” of information.<sup>26</sup>

## Authenticity

In the context of an advanced neuroprosthetic system, we can define authenticity as **“the quality of in fact deriving from the same source or origin that is claimed or supposed to be the information’s source or origin.”**

For example, the human host and user of a set of two artificial eyes might reasonably assume that the visual sense data presented by the eyes represents an accurate depiction of the physical environment surrounding the eyes’ host. If the artificial eyes are presenting the host with the visual experience that he is sitting in his office at work while in fact he has been kidnapped and is sitting in a laboratory in the headquarters of a rival company – with his artificial eyes having been hacked to provide him with a false impression of his surroundings – we could say that the information being provided by the artificial eyes is inauthentic.<sup>27</sup>

On the other hand, if – as an alternative means of taking a “vacation” – a neuroprosthetic device’s host had purposefully paid a sensory engineer to provide him with the visual experience of lounging on a tropical beach while in fact he was lying on his couch at home, we might say that this experience was “virtual” or “fabricated,” but according to our definition it would not be “inauthentic,” because the host knew that the source of his sense data was not an actual physical beach surrounding him.<sup>28</sup> In other words, the host would not be having an experience of lounging on a real beach that is inauthentic but rather an authentic experience of lounging on a virtual beach.

---

<sup>25</sup> Parker, “Toward a New Framework for Information Security” (2002), p. 125.

<sup>26</sup> Dardick, “Cyber Forensics Assurance” (2010), p. 61.

<sup>27</sup> For the possibility that a device designed to receive raw data from the external environment could have that data replaced with other data transmitted from some external information system, see Koops & Leenes, “Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes” (2012). Regarding the possibility of neuroprosthetics being used to provide false data or information to their hosts or users, see also McGee, “Bioelectronics and Implanted Devices” (2008), p. 221.

<sup>28</sup> In a similar way, one might say that a novel which claims to be historically accurate but is full of errors and anachronisms is “inauthentic,” while the same work – if explicitly marketed as a work of fantasy and creative fiction – could not be criticized for being “inauthentic.”

Note that according to our definition, in order for some information provided by a neuroprosthetic device to be inauthentic it is not necessarily required that someone has *explicitly claimed* that this particular information is accurate or originates from a source that is not its actual source; it is enough for the device's host or user to *suppose* that the information is originating from some source which is, in fact, not the actual source of the data. If a particular neuroprosthetic device was sold without any claim that it will provide accurate and authentic information, but its human user has utilized the device for some time and has always found it to present an accurate and authentic representation of the physical environment surrounding the user, then the user might understandably come to assume that this will always be the case in the future. If the device were then hacked and began to present the user with a stream of sense data that was inaccurate and did not reflect physical reality, that information could well be described as "inauthentic," from the user's perspective.

Gray areas may especially arise when neuroprosthetics are being purposefully used to immerse their users in fabricated virtual environments. In general, it is more difficult to describe the information presented by a device as "inauthentic" if the user knows that the purpose of the device is to present a fabricated virtual experience, however it is still possible. For example, imagine that all of a multinational company's employees use neuroprosthetic devices that create a shared virtual environment in which employees from around the world can interact. If a hacker were to manipulate the sense data provided to one particular employee so that he or she believed that a coworker had just made a statement within the virtual world which, in fact, the coworker had never made, the contents of that fabricated statement could be understood as inauthentic.

Within the classic CIA Triad, authenticity is not explicitly described as a security goal. It is included in the expanded Parkerian Hexad, where authenticity is defined as the "Validity, conformance, and genuineness of information."<sup>29</sup> Dardick's synthetic CFA model, meanwhile, summarizes the joint concept of "Authenticity/Original" as the "quality of being authentic or of established authority for truth and correctness – 'best evidence' (Validity)."<sup>30</sup>

## Utility

With regard to an advanced neuroprosthetic system, we can define utility as **"the state of being well-suited to be employed for a chosen purpose."**

---

<sup>29</sup> Parker, "Toward a New Framework for Information Security" (2002), p. 125.

<sup>30</sup> Dardick, "Cyber Forensics Assurance" (2010), p. 61.

Information is not inherently useful or non-useful; it possesses utility only with regard to some particular purpose that has been chosen by a sapient agent, such as its human host or user. The same information could be useful to one person in one moment but not useful to a different person or in a different moment.

For example, an artificial eye might generate sense data that is of use to its human host in navigating his or her environment, reading, working at a computer, cooking, or carrying out countless other everyday activities but which is not useful (and may even be distracting and detrimental) if the user is attempting to meditate, sleep, or concentrate on some mental task. Moreover, the device itself ceases to generate information that is even potentially useful when the eyelids in front of it are closed.<sup>31</sup> Other kinds of advanced neuroprosthetics might not generate any information that is immediately useful to their host but may generate vast quantities of biological and diagnostic data that is useful to the team of medical personnel or engineers who are monitoring and controlling a device in order to effectuate some particular outcomes.

The concept of utility is not explicitly incorporated into the classic CIA Triad – though information’s potential utility could be understood, for example, as the reason *why* one wishes certain information to be “available.” Dardick’s synthetic CFA model summarizes the joint concept of “Utility/Relevance” as providing an answer to the question “Is it useful? / is it the right information?”<sup>32</sup> As part of his security hexad, Parker defines utility as the “Usefulness of information for a purpose”<sup>33</sup> – which in the case of an advanced neuroprosthetic could be a purpose defined by the device’s human host, by medical personnel or “experiential engineers” who maintain and control the device with the host’s permission in order to produce particular effects for the host, or potentially by an individual or organization that has installed the neuroprosthetic without its host’s knowledge or permission and which is utilizing the device to advance objectives that it has determined. The latter might be the case, for example, with a neuroprosthetic that is implanted in an infant at the request of its parents, in a comatose individual at the request of his or her guardian, or by a government agency into its military personnel or corporation into employees. In such cases, the questionable legality and

---

<sup>31</sup> Even with the eyelids closed, an artificial eye conveys very basic information about whether the external environment surrounding the host is pitch black, moderately illuminated, or brightly illuminated. In some cases it may be desirable to eliminate the eyelids’ ability to close (e.g., in order to blink or while the host is asleep) in order to allow images recorded by the eyes to be stored or transmitted, even if they are not immediately consciously experienced or used by the host himself or herself.

<sup>32</sup> Dardick, “Cyber Forensics Assurance” (2010), p. 61.

<sup>33</sup> Parker, “Toward a New Framework for Information Security” (2002), p. 125.

ethicality of such operations is not being considered here, only the fact that regardless of by whom or for what purpose a neuroprosthetic has been implanted, the party who has implanted it will see the device's ongoing utility as an objective to be pursued and whose loss would compromise the device's information security.

## Distinguishability

In the context of an advanced neuroprosthetic system, we can define distinguishability as **“the ability to differentiate the information to be secured from information possessing a different source or nature.”**

In the case of a desktop computer, laptop computer, or mobile device, it is relatively easy to distinguish the system and data whose information security one is seeking to ensure: such devices are discrete units that can be identified and physically separated from their environments. Moreover, it is relatively easy to identify what data is stored on the device, whether it be stored on a magnetic hard drive, flash memory, ROM, or some other physical substrate. By knowing the boundaries of one's system and identifying the information that is to be protected, one can thus develop a clear information security strategy. However, because of their close integration with the human body and human mind's own systems for generating, receiving, storing, transmitting, and processing information, it can be difficult to determine: 1) which are the synthetic systems and neuroprosthetically derived information which the designer, manufacturer, and operator of a neuroprosthetic device may possess the legal and ethical authority to control and manipulate (and for whose security they may bear both legal and ethical responsibility), and 2) which are the natural systems and informational content of the host's biological body and mind – which the operator of a neuroprosthetic device may have a legal and ethical responsibility to keep secure, but without necessarily possessing a legal basis for controlling, manipulating, or even affecting those systems and sources of information.<sup>34</sup> If the information provided by a neuroprosthetic cannot be distinguished from information emanating from other sources, it likely becomes more difficult to ensure the information's security.

Consider a human being who has been implanted with retinal implants that supply the visual sense data constituting 30% of the person's field of vision, while the remaining 70% of the sense data is provided by the person's natural retinal cells. If the person knows which 30% of his field of vision is

---

<sup>34</sup> In respect to the complex questions that arise regarding who bears moral, legal, and financial responsibility for activities involving implanted ICT devices, see Roosendaal, “Carrying Implants and Carrying Risks; Human ICT Implants and Liability” (2012).

being generated by his neuroprosthetics, his information security situation is qualitatively different from that of a person who knows that 30% of his field of vision is being provided by an artificial device but does not know *which portion* of his field of vision is “synthetic” and which is “natural.” Similarly, the user of a mnemocybernetic implant who is able to easily distinguish (e.g., through some ineffable inner sensation or awareness) the mnemonic content provided by the implant from the mnemonic content stored in his or her brain’s natural memory systems faces a different information security situation than someone who knows that he or she possesses a mnemonic implant but has no way of distinguishing memories stored in the implant from memories stored in the natural mechanisms of his or her brain – and different still is the situation of someone who does not even realize that he or she possesses a mnemonic implant and who is not even aware that he or she should be *attempting* to distinguish between those memories that are natural and those that are neuroprosthetically generated.

## Rejectability

With regard to an advanced neuroprosthetic system, we can define rejectability as **“the ability to exclude particular information from one’s conscious awareness on the basis of its source, nature, or other characteristics.”**

It is important to ensure that information is available whenever its user wishes to access it. However, in the case of a neuroprosthetic device it is at least as important to ensure that the information is not involuntarily forced into the mind of its host or user when he or she *does not* wish to access it.

The ability of advanced neuroprosthetics to forcibly inject experiences – whether sense data, memories, emotions, or other mental phenomena – into the conscious awareness of their host or user makes it essential that such devices have safeguards to guarantee that their users are not subject to sensory overload, brainwashing, or other kinds of psychological or emotional assault. This becomes particularly important if, for example, a neuroprosthetic device has been implanted in a child, an individual suffering motor impairments, or other persons who may not be able to actively adjust or disable the device or express their lack of consent to the experience. Cognitive security involves not only being able to bring desired information into one’s mind for use but also to keep it out of one’s mind, when desired.

## Autonomy

In the context of an advanced neuroprosthetic system, we can define autonomy as **“the state of a subject that consciously experiences its own use of information and which possesses and exercises agency in generating information.”**

This is clearly not an attribute that applies to information stored in a traditional system, such as the hard drive of a desktop computer. In that case neither the information itself nor the computer system containing the information possesses a subjective experience of the information, and if the computer can be said to exercise “agency” in generating information, it is only in a limited sense (at least, in comparison to human beings), insofar as a conventional computer does not possess its own desires, beliefs, volitions, or conscience.<sup>35</sup>

In the case of a human being implanted with an advanced neuroprosthetic device, the information contained within the device does not, in itself, possess autonomy. However, unless he or she is in a comatose state and thus deprived of the ability to consciously experience information or utilize agency in generating it, the potential human host of a neuroprosthetic device *does* possess informational autonomy in the sense defined above, and the integration of the neuroprosthetic device into the host’s neural circuitry to create a new device-host system should not be allowed to impair or destroy the host’s informational autonomy. In this sense, we can say that preserving the informational autonomy of the device-host system is an important goal of information security. Autonomy is thus the epitome of a new kind of security goal and attribute that has not been relevant for the information security of traditional computerized data-storage systems but which becomes relevant – and, indeed, assumes paramount importance – in the case of information stored within an advanced neuroprosthetic and the system that it forms with its human host.

When working to ensure the security of information contained within a hard drive, the hard drive does not possess its own rights or human welfare about which we must be concerned. Similarly, a computer running the most sophisticated sorts of artificially intelligent software available today may demonstrate a limited form of agency, but such a platform is not a moral agent that is capable of possessing its own conscience (or “metavolution”) or conscious awareness, nor is it (like infants or at least some animals) the sort

---

<sup>35</sup> For the extent to which it is possible for technological devices – whether a conventional desktop computer or a far more sophisticated construct such as a social robot or artificial general intelligence (AGI) – can possess and demonstrate agency and autonomy and the forms that these traits can take, see, e.g., Coeckelbergh, “From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots” (2011); Calverley, “Imagining a non-biological machine as a legal person” (2008); Hellström, “On the Moral Responsibility of Military Robots” (2013); Kuflik, “Computers in Control: Rational Transfer of Authority or Irresponsible Abdication of Autonomy?” (1999); Stahl, “Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency” (2006); and Friedenberg, *Artificial Psychology: The Quest for What It Means to Be Human* (2011).

of “moral patient” about whose welfare human beings must be concerned even though it is not in itself a moral agent. Thus in certain circumstances it may be appropriate to destroy a hard drive or computer as part of an overall strategy for keeping secure the information contained within it. However, in the case of a neuroprosthetic device, maintaining the biological and psychological welfare of the being into whose organism and mind the device is integrated is typically the greatest priority, and any efforts at securing the neuroprosthetic device and information contained within it must not be allowed to impair the wellbeing of the device’s human host.

Note that there is not simply a danger that a device’s built-in information security mechanisms might harm its host; it is also possible that the device’s mere presence might damage the mind of its host and the information contained within that mind. Especially in the case of neuroprosthetics that affect their host’s processes of memory,<sup>36</sup> volition, metavolition,<sup>37</sup> emotion,<sup>38</sup> and conscious awareness,<sup>39</sup> there is a possibility that the device might negatively impact the host’s possession and exercise of the autonomy, moral agency, consciousness, and conscience that are among the defining traits of a human being.

It is possible to conceive of an invasive neuroprosthetic device which, for example, replaces sections of the host’s brain in a way that destroys the host’s conscious awareness while replacing it with an AI-driven artificial agency contained in the device.<sup>40</sup> Such concerns regarding authenticity and personal identity have already been expressed regarding neural implants used for deep brain stimulation to treat conditions such as Parkinson’s disease.<sup>41</sup> We can

---

<sup>36</sup> For the possibility of developing mnemoprosthetics, see Han et al., “Selective Erasure of a Fear Memory” (2009), and Ramirez et al., “Creating a False Memory in the Hippocampus” (2013).

<sup>37</sup> See, for example, Negoescu, “Conscience and Consciousness in Biomedical Engineering Science and Practice” (2009), and Gladden, “Tachikomatic Domains: Utopian Cyberspace as a ‘Contingent Heaven’ for Humans, Robots, and Hybrid Intelligences” (2015).

<sup>38</sup> For the possibility of developing emotional neuroprosthetics, see Soussou & Berger, “Cognitive and Emotional Neuroprostheses” (2008); Hatfield et al., “Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior” (2009); Kraemer, “Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation” (2011); McGee, “Bioelectronics and Implanted Devices” (2008), p. 217; and Fairclough, “Physiological Computing: Interfacing with the Human Nervous System” (2010).

<sup>39</sup> For the possibility of neuroprosthetic devices relating to sleep, see Claussen & Hofmann, “Sleep, Neuroengineering and Dynamics” (2012), and Kourany, “Human enhancement: Making the debate more Productive” (2013), pp. 992–93.

<sup>40</sup> See Gladden, “Tachikomatic Domains: Utopian Cyberspace as a ‘Contingent Heaven’ for Humans, Robots, and Hybrid Intelligences” (2015), and Gladden, “Upgrading’ the Human Entity...” (2015).

<sup>41</sup> For the effects of existing kinds of neuroprosthetic devices on the agency (and perceptions of agency) of their human hosts, see Kraemer, “Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation” (2011), and Berg, “Pieces of Me:



summarize these concerns and this security goal by stating that a neuroprosthetic device should support rather than impair the autonomy of its human user.

## Prioritizing the information security goals

Parker notes that – however many security attributes one might define – they should be placed in some logical order (such as their order of importance) that adds an additional level of meaning to the list of attributes.<sup>42</sup> If we were to arrange our nine security goals in order of importance as seen from the perspective of a generic neuroprosthetic device-host system (and in particular, a host’s conscious awareness), a ranking that appears reasonable would be:

- **Autonomy** of the device-host system, insofar as a neuroprosthetic device and system that impairs its host’s autonomy, agency, conscience, and conscious awareness may actually destroy the most fundamental ability of its hostmind to experience and use information, thereby rendering all of the other security attributes irrelevant.
- **Rejectability**, as the ability of a hostmind to *block out* a stream of information that is causing ongoing pain, sensory overload, or physical or psychological trauma is arguably more important than the mind’s ability to *access* information that is beneficial and useful.
- **Integrity**, which, if lost, would likely diminish or destroy information’s utility and authenticity and render possession of the information of little value.
- **Utility**, as there is little need to ensure, e.g., the availability or possession of information if it is ultimately of no use to the neuroprosthetic device’s user.
- **Availability**, which may be crucial for information provided by some neuroprosthetics (e.g., sense data provided by an artificial eye should be in real time, in order to synchronize with data provided by other sensory organs and allow real-time motor control) but less important for information provided by others (e.g., a delay in pulling up certain kinds of long-term memories stored in a memory implant may be permissible).

---

On Identity and Information and Communications Technology Implants” (2012).

<sup>42</sup> Parker, “Our Excessively Simplistic Information Security Model and How to Fix It” (2010), p. 17.

- **Confidentiality**, insofar as a neuroprosthetic device may potentially allow outside agents to access the contents of its user's volitions, memories, emotions, and other intimate mental processes whose contents the user would very much like to keep private.
- **Authenticity**, insofar as information that is "false" or "inauthentic" (e.g., fabricated sense data that intentionally misleads the device's user into believing that he is walking through a forest while in fact he is lying on a bed in a hospital) may still be of great value to the device's host and operator as long as it is useful and available.
- **Possession**, as the long-term holding and control of some information provided by neuroprosthetics (such as long-term memories) may be important, but the ability to store long-term and to control of other kinds of information (such as a complete permanent record of all the visual information that one has experienced through one's retinal implants) that are generally experienced by the mind only instantaneously is something that human beings do not currently enjoy and may not expect.
- **Distinguishability**, insofar as it may not be important to distinguish neuroprosthetically supplied from naturally supplied information, as long as the neuroprosthetically supplied information possesses all of the other security attributes. However, distinguishability becomes an important tool that is useful for pursuing information security in cases where other attributes are lacking and specific vulnerabilities, threats, or risks need to be addressed.

Note that if one accepts this ordering, two of the three new security goals for advanced neuroprosthetics that have been introduced in this chapter turn out to be more important than any of the goals traditionally defined in the CIA Triad and Parkerian Hexad. This highlights the danger of assuming that security goals that were developed with previous standalone computer systems (e.g., desktop or laptop computers) in mind will provide an adequate basis for ensuring information security for new kinds of neuroprosthetic devices that are intimately interconnected with the biological and mental processes of a human user. This underscores the need to develop new and more robust "cognitive security frameworks" for such brain-machine interfaces.

Although the ranking of security attributes just proposed appears reasonable as a generic approach, many alternative rankings are possible. While Parker seems to suggest that there may be a single most logical way of ordering

security attributes,<sup>43</sup> other experts note that different organizations will prioritize security attributes in different ways,<sup>44</sup> based on each organization's unique mission and the role that information and information technology play within it. In the case of an advanced neuroprosthetic system, any prioritized ordering of security attributes includes many implicit value judgments about the relative importance of various objectives, and different individual hosts or users of neuroprosthetic implants might rank the attributes in quite different ways.

For example, for some device hosts who are powerful political figures or business leaders, ensuring the confidentiality of information contained within their minds might be the ultimate priority, insofar as that information may include classified national security plans that must not be allowed to fall into the hands of hostile states or trade secrets that could be exploited by competing firms; moreover, the person's mind may contain information (e.g., long-term memories dating back to childhood) which, if acquired by unauthorized parties, could provide a basis for blackmail, extortion, or other illicit manipulation. On the other hand, other users might be willing to accept a loss of confidentiality, if in return their neuroprosthetics would grant them new sensorimotor or cognitive capacities, allow them to interact socially in new ways, or provide them with other advantages that outweigh the loss of confidentiality. Indeed, there is even reason to believe that over time, some human beings may come to embrace the use of neuroprosthetics that allow members of a community to mutually experience one another's thoughts – thereby purposefully reducing the confidentiality of information contained within their minds in order to forge new kinds of political dialogue and social relations; in such cases, a loss of confidentiality could be experienced as something “liberating” that advances openness and honesty rather than something frightening and oppressive.<sup>45</sup>

Similarly, some users may give paramount value to the authenticity of the information being conveyed by their neuroprosthetic device. Such users might prefer to have an artificial eye which, for example, provides them with a stream of low-resolution visual sense data that is not particularly useful but which they know is “authentic” (i.e., it accurately reflects the objective physical reality of the environment surrounding them) rather than to possess an artificial eye that provides flawless high-resolution video but which can easily

---

<sup>43</sup> Parker, “Our Excessively Simplistic Information Security Model and How to Fix It” (2010), p. 17.

<sup>44</sup> *NIST SP 800-33* (2001), p. 2.

<sup>45</sup> See Gladden, “‘Upgrading’ the Human Entity...” (2015).

be hacked by unauthorized parties – so that the device’s user never knows whether the world that they are seeing actually exists or whether it is a false or virtual environment that they are experiencing as a result of fabricated sense data that is being fed to their neuroprosthetic device by a malicious hacker.

When prioritizing the information security goals for a particular advanced neuroprosthetic system, the system’s designer should thus take into account factors such as:

- The **market segment(s) of potential users** at whom the device is being targeted.
- The unique information security **needs and concerns** displayed by those groups.
- The ways in which the information security characteristics of the neuroprosthetic device itself, physical maintenance services, software updates, and other products and services offered by the manufacturer will **integrate with the existing information security systems**, services, and priorities maintained by institutions (such as an employer, school, health care provider, or government agency) that already bear responsibility for ensuring those users’ information security.

Moreover, in order for the potential user of a neuroprosthetic device to choose the device that is best for him or her and to provide informed consent for its implantation, the relative prioritization of information security goals that have been incorporated into the device’s design and functioning should be disclosed to the potential user in the relevant marketing materials and pre-implantation counseling.

## Understanding the security goals at three levels

The human host of an advanced neuroprosthetic device intertwines his or her personal informational security with that of the system on different levels, each of which has distinct information security challenges and characteristics

that must be taken into consideration.<sup>46</sup> We must consider the neuroprosthetically enabled human being on at least three different levels:<sup>47</sup>

- 1) The human being as a **sapient metavolitional agent**, a unitary mind that possesses its own conscious awareness, memory, volition, and conscience (or “metavolitionality”<sup>48</sup>)).
- 2) The human being as an **embodied embedded organism** that inhabits and can sense and manipulate a particular environment through the use of its body.
- 3) The human being as a **social and economic actor** who interacts with others to form social relationships and to produce, exchange, and consume goods and services.<sup>49</sup>

---

<sup>46</sup> Note that while considering the human host of a neuroprosthetic device separately as a sapient mind, embodied biological organism, and social and economic actor is useful for ensuring that one does not overlook any of the information security issues that become especially apparent when considering the human host in one of those capacities, in reality these three roles are always fused and deeply interrelated, if not wholly inextricable from one another. In future posthuman contexts in which very sophisticated neuroprosthetic devices have been deployed, it may sometimes be clear, for example, that a particular human being has become “infected” by a particular *idée fixe* that occupies all of his or her thoughts or wrapped up in a relationship (such as one of love, loyalty, or hatred) that consumes all of the person’s energy and attention – but it may be unclear whether the source of the phenomenon – the “vector” that introduced it into the person’s life and being – was a biological vector (such as a biological virus or biochemical agent that has affected the person neurologically or physiologically), an electronic vector (such as glitches that occurred in the gathering of sense data or storage of memories by an implant or a computer worm or virus that has infected the synthetic components of the device-host system), or a social vector (such as acts of inspiration, persuasion, seduction, blackmail, or myth-building performed by other intelligent agents and directed at the person). For a use of actor-network theory (ANT) to explore the ways in which, for example, a single “idea” might manifest itself through diverse biological, mental, technological, and social phenomena or activity and the complexities involved with untangling biological and technological symbioses and power relations within such a posthuman context, see Kowalewska, “Symbionts and Parasites – Digital Ecosystems” (2015).

<sup>47</sup> See Gladden, “Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems” (2015). The reminder of this chapter draws heavily on that work.

<sup>48</sup> See Calverley, “Imagining a non-biological machine as a legal person” (2008), for an explanation of the relationship of second-order volitions to conscience and Gladden, “Tachikomatic Domains: Utopian Cyberspace as a ‘Contingent Heaven’ for Humans, Robots, and Hybrid Intelligences” (2015), for use of the word “metavolitional” in this context regarding to neuroprosthetic devices.

<sup>49</sup> The financial and economic aspect of a neuroprosthetic device’s impact is important, insofar as financial considerations influence the kind and degree of security measures that can be implemented by individual or institutional users of neuroprosthetic devices, and efforts to compromise information security and illicitly acquire information often have a financial component (e.g., as part of a planned scheme for blackmail, corporate espionage, or sale of the information).

At each of these three levels, a neuroprosthetic device integrates with its host's own natural capacities to create a device-host system whose unique characteristics may create powerful new tools that can assist with ensuring the system's information security, dramatic new vulnerabilities that undermine the system's information security, or both. Below we consider some new capacities and limitations that a neuroprosthetic device can provide its human host at each of the three levels and describe the impact that these new characteristics can have on pursuit of the nine security goals.

### Functional vs. information security impacts

Note that there is no direct correlation between a neuroprosthetic device having an *overall functional impact* on its host that is considered positive or negative and its having a more specific *information security impact* that is considered positive or negative. Some of the new neuroprosthetically facilitated characteristics which might be considered *beneficial* from the host or user's perspective (due to the new functional capacities that they provide) may be considered harmful and disadvantageous from the perspective of the InfoSec professionals who are charged with ensuring the host's information security, insofar as the characteristics create egregious new vulnerabilities. Conversely, some feature of a neuroprosthetic device that is generally considered undesirable from the perspective of its host (because it limits or constraints the host in some way) might be considered advantageous from an information security perspective, insofar as it provides a new layer of defense that protects information contained within the host's biological systems or mental processes from access by unauthorized parties.

### Impacts on a host vs. impacts on a user

Note also that the impacts that a particular neuroprosthetic device has on the information security of its human *host* may differ significantly (and even be diametrically opposed to) the impacts that it has on the information security of its operator or *user*, if the host and user are different persons. In cases where the host and user are different individuals, this cognitive security framework should be applied separately to the device's host and its user and due attention should be paid to the impacts result for each person.

### The human host as sapient metavolitional agent

**FUNCTIONAL CAPACITIES CREATED BY A NEUROPROSTHETIC DEVICE**

Below we describe some of the new functional capacities that a neuroprosthetic device can provide its host or user in his or her role as a sapient metavolitional agent and the potential impact that these capacities might have on the information security of the host-device system.<sup>50</sup>

***Enhanced memory, skills, and knowledge stored within the mind (engrams)***

Building on current experimental technologies that are being tested in mice, future neuroprosthetics may offer human users the ability to create, alter, or weaken memories that are stored in their brains' natural memory systems in the form of engrams.<sup>51</sup> This could potentially be used not only to affect a user's declarative knowledge but also to enhance motor skills or reduce learned fears.

Tremendous technological challenges would need to be overcome in order to someday develop a neuroprosthetic device that allows for the precise "editing" of extant human memories or creation of complex new memories within the brain's naturally existing memory systems. Indeed, the exact structures and processes used by the brain to encode, store, and retrieve long-term memories are still shrouded in mystery, and researchers have proposed divergent theories to account for the way in which the brain stores engrams.<sup>52</sup> If, for example, a model such as the Holonomic Brain Theory is correct, then any efforts to make precise adjustments to existing memories by manipulating neurons in a particular portion of the brain may prove futile, as each memory may be stored holographically across the brain's entire neural network.<sup>53</sup> Although researchers have succeeded in understanding many of the large-scale synaptic structures and basic electrochemical functioning of neural synapses – and are making rapid progress at developing artificial neurons that can replicate key elements of this observed synaptic functioning – there is still considerable debate about the extent to which these simple, large-scale

---

<sup>50</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>51</sup> See Han et al., "Selective Erasure of a Fear Memory" (2009); Ramirez et al., "Creating a False Memory in the Hippocampus" (2013); McGee, "Bioelectronics and Implanted Devices" (2008); and Warwick, "The cyborg revolution" (2014), p. 267.

<sup>52</sup> See, for example, Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

<sup>53</sup> See Longuet-Higgins, "Holographic Model of Temporal Recall" (1968); Pribram, "Prolegomenon for a Holonomic Brain Theory" (1990); and Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web..." (1999).

synaptic structures and actions within the brain are responsible for the creation, storage, and recall of long-term memories.<sup>54</sup> Elements of the Holonomic Brain Theory, for example, suggest that much more sophisticated and difficult to observe interactions between neurons (such as those within the “synaptodendritic web”<sup>55</sup>) – may play essential roles in the memory process that we have barely begun to comprehend. The development of a neuroprosthetic device that can successfully integrate with the brain’s neural circuitry in order to support, expand, control, or replace the brain’s natural mechanisms for creating, storing, and recalling complex engrams is not expected to occur soon, and – depending on which theories of the brain’s memory processes prove correct – it may not even be theoretically possible at all.

However, if one assumes that such a technology could be developed, it is clear that it would have major implications for the security of information held within the long-term memory of its host and user. If a device allowed external agents to access and copy the mind’s engrams, this would imperil that information’s **confidentiality** as well as the host’s **possession** of it. The ability to edit or delete existing engrams would threaten the information’s **integrity**, **utility**, **availability**, and **authenticity** for the host. If the device were able to forcibly recall particular memories to the host or user’s conscious awareness against his or her will, it would undermine the **rejectability** of that information. If the device gave an external agent the wholesale ability to delete, replace, or manipulate the host’s memories, this could potentially reduce the host’s **autonomy** by eliminating his or her own ability to exercise agency in generating mnemonic contents. If the device were integrated seamlessly into the brain’s natural mnemonic systems, from the host and user’s perspective the (potentially inauthentic) memories generated by the neuroprosthetic device might lack **distinguishability** from natural memories that were generated by some actual experience in the host’s past.

### ***Enhanced creativity***

A neuroprosthetic may be able to enhance a mind’s powers of imagination and creativity<sup>56</sup> by facilitating processes that contribute to creativity, such as stimulating mental associations between unrelated items. Anecdotal increases in creativity have been reported to result after the use of neuroprosthetics for deep brain stimulation.<sup>57</sup>

---

<sup>54</sup> For example, see Dudai, “The Neurobiology of Consolidations, Or, How Stable Is the Engram?” (2004).

<sup>55</sup> See Pribram & Meade, “Conscious Awareness: Processing in the Synaptodendritic Web...” (1999).

<sup>56</sup> See Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012), pp. 23-24.

<sup>57</sup> See Cosgrove, “Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation” (2004), and Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement”



If such a device were able to force new thoughts into its host's mind against his or her will, that information would lack **rejectability**, and the device might undermine **autonomy** by interfering with or overriding the host's ability to generate his or her own creative thoughts. Moreover, by forcing unwanted and distracting memories into the host's conscious awareness, this could interfere with the host's efforts to access *other* information contained within his or her memory, thereby reducing the **availability**, **utility**, and potentially **integrity** of the latter information. If the host could never be sure whether new ideas had been generated by his or her own imagination or by the device, those ideas would lack **distinguishability**. The ability of outside agents to access ideas generated by the device would undermine that information's **confidentiality** and the host's **possession** of it.

#### ***Enhanced emotion***

A neuroprosthetic device might provide its host with more desirable emotional dynamics and behavior.<sup>58</sup> Effects on emotion have already been seen, for example, with devices used for deep brain stimulation.<sup>59</sup>

If such a device allowed external agents to detect the host's internal emotional states, the device would be undermining the user's **possession** and the **confidentiality** of that information. If the device could force emotional content into the host's conscious awareness, that information would lack **rejectability** and could undermine the host's **autonomy**. Insofar as such involuntary emotional dynamics distort or render impossible the host's ability to efficiently access and use other information, the **availability**, **utility**, and perhaps **integrity** of such information would suffer.

On the other hand, in the case of a host whose previous severe emotional disturbances had made it difficult or impossible for the person to calmly and efficiently access utilize information contained within his or her memory or provided by the external environment, the use of such a device could potentially *enhance* the **availability** and **utility** of such information. If a person is prone to fits of uncontrollable anger, jealousy, or pride during which he or she lashes out and reveals his or her deepest and harshest criticisms of others or other personal secrets, the use of a neuroprosthetic device to limit such frustrations and outbursts could aid the person in maintaining the **confidentiality** and **possession** of information which, in moments of greater rationality,

---

(2012).

<sup>58</sup> McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>59</sup> See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011).

the person would admit that he or she has no desire to reveal. By giving the user greater control over his or her emotions, such a device could enhance the person's own agency (and thus informational **autonomy**) and increase the **rejectability** of unwanted thoughts and feelings that the user was previously unable to block out of his or her mind.

#### *Enhanced conscious awareness*

Research is being undertaken to develop neuroprosthetics that would allow the human mind to, for example, extend its periods of attentiveness and limit the need for periodic reductions in consciousness (i.e., sleep).<sup>60</sup>

By enhancing the mind's attentiveness and ability to spend extended periods of time focused on accessing and processing information, such a device could indirectly enhance the **availability** and **utility** of information for its host. Enhancing and extending the host's conscious awareness could also temporarily expand (if not otherwise qualitatively change) the host's ability to exercise agency and **autonomy** in the accessing and use of information. On the other hand, if the device is capable of forcibly compelling the host to focus his or her conscious awareness on a particular piece of information, that would limit the **rejectability** of that information and weaken the host's **autonomy**. Moreover, if the device could be misused to *reduce* the host's conscious awareness, this would impair his or her ability to subjectively experience information and thus reduce the host's **autonomy**.

#### *Enhanced conscience*

If a "volition" is understood as a belief about the outcome of some action and a desire for that outcome,<sup>61</sup> then one's conscience can be understood as one's set of second-order volitions or "metavolitions," desires about the kinds of volitions that one wishes to possess.<sup>62</sup> Insofar as a neuroprosthetic device enhances processes of memory and emotion<sup>63</sup> that allow for the development of one's conscience, the device may enhance one's ability to develop, discern, and follow one's conscience.<sup>64</sup>

A neuroprosthetic device that is capable of altering a host's most fundamental desires and assessment of what is "right" and "wrong" would have major implications for information security – most noticeably in either strength-

---

<sup>60</sup> Kourany, "Human enhancement: Making the debate more Productive" (2013), pp. 992-93.

<sup>61</sup> Calverley, "Imagining a non-biological machine as a legal person" (2008), pp. 528-30.

<sup>62</sup> See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

<sup>63</sup> Calverley, "Imagining a non-biological machine as a legal person" (2008), pp. 532-34.

<sup>64</sup> See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

ening or undermining the host's informational **autonomy** and potentially impairing the **integrity** and **availability** of the information that would be conveyed by the host's unaugmented conscience in the absence of such a device. By affecting the host's metavolitions, such a device would over time alter the **rejectability** and availability of information contained in the host's first-order volitions. If such a device provides the host with metavolitions that are determined by (and thus known to) some external agency, the host's previous metavolitions (over which he or she presumably exercised **possession** and sole control) would be replaced by new metavolitions lacking **confidentiality** and sole **possession** by the user.

#### **FUNCTIONAL IMPAIRMENTS CREATED BY A NEUROPROSTHETIC DEVICE**

Below we describe some of the functional impairments that a neuroprosthetic device might create for its host at the level of his or her internal mental processes and the impact that these impairments might have on the information security of the host-device system.<sup>65</sup>

##### ***Loss of agency***

A neuroprosthetic may damage the brain or disrupt its activity in a way that reduces or eliminates the ability of its human user to possess and exercise agency.<sup>66</sup> Moreover, the knowledge that this can occur may lead users to doubt whether their volitions are really "their own," an effect that has been seen with neuroprosthetics used for deep brain stimulation.<sup>67</sup>

A neuroprosthetic device that produces a general loss of agency would clearly have a negative impact on its host's informational **autonomy** by reducing the host's ability to possess and exercise agency in generating information. It could also indirectly reduce the **rejectability** of unwanted information and the **availability** of desired information.

##### ***Loss of conscious awareness***

A neuroprosthetic may diminish the quality or extent of its host's conscious awareness, e.g., by inducing daydreaming or increasing the required amount of sleep. A neuroprosthetic could potentially even destroy its user's

---

<sup>65</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>66</sup> McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>67</sup> See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011).

capacity for conscious awareness (e.g., by inducing a coma) but without causing the death of his or her biological organism.<sup>68</sup>

A neuroprosthetic device that produces a loss of conscious awareness on the part of its host would have a negative impact on its host's informational **autonomy** similar to that produced by a loss of agency; if the host's ability to subjectively experience information is completely destroyed, then other attributes such as the **integrity**, **utility**, and **availability** of information for that host would become largely irrelevant, as there would no longer be a "host" to whom the information could be presented.

#### *Dependency of internal cognitive processes on external systems*

Although the portion of a neuroprosthetic device that directly interfaces with its host's neural circuitry may be implanted in the host's body, it is possible that internal processing, memory, and power constraints may force the device to regularly offload some information to an external system for processing (e.g., through a wireless data link) or to receive instructions from the external system; in this way, the "internal" cognitive processes of the device's host may no longer be taking place solely within the relatively easily protected space of the host's brain and body but within an array of physically disjoint systems that communicate through channels that may be subject to accidental disruption or intentional manipulation.

The restructuring of the host's cognitive processes in such a way increases the possibility of a loss of **autonomy** and reduction in the **integrity**, **availability**, **confidentiality**, **authenticity**, and **possession** of information contained in those cognitive processes. On the other hand, use of external systems to support or create a "backup copy" of the host's internal cognitive processes could potentially also aid in the diagnosis and treatment of cognitive disorders, increased efficiency and power in the mind's cognitive processing, and the restoration of information that otherwise would have been lost to or by the brain's internal cognitive processes – all of which might contribute to an increase in **autonomy** and the **integrity**, **availability**, and **utility** of information.

#### *Inability to distinguish a real from a virtual ongoing experience*

If a neuroprosthetic device alters or replaces its host's sensory perceptions, it may make it impossible for the user to know which (if any) of the sense data that he or she is experiencing corresponds to some actual element of an external physical environment and which is "virtual" or simply "false."<sup>69</sup>

<sup>68</sup> See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

<sup>69</sup> For the possibility that a device designed to receive raw data from an external environment could have that data replaced with other data transmitted from some external information system, see Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Ad-

Such a neuroprosthetic device would certainly produce a loss of **distinguishability** in the sensory information experienced by its host and would open the door to external manipulation that could reduce the **availability** of accurate information that the host was blocked from seeing and the **authenticity** and **utility** of the information that was instead received by the host.

#### *Inability to distinguish true from false memories*

If a neuroprosthetic device is able to create, alter, or destroy engrams within its host's brain, it may be impossible for a host to know which of his or her apparent memories are "true" and which are "false" (i.e., distorted or purposefully fabricated).<sup>70</sup>

This kind of neuroprosthetic device would produce a loss of **distinguishability** in the mnemonic information experienced by the host and could facilitate external manipulation that could reduce the **availability** of accurate mnemonic information that the host was blocked from recalling and the **authenticity** and **utility** of the information that was instead recalled by the host. It could also impair the host's **autonomy**, insofar as he or she may be exercising agency and making decisions based on memories that are not actually his or her own.

#### *Other psychological side-effects*

A host's brain may undergo potentially harmful and unpredictable structural and behavioral changes as it adapts to the presence, capacities, and activities of an advanced neuroprosthetic device.<sup>71</sup> These effects may even include new kinds of neuroses, psychoses, and other disorders unique to hosts or users of advanced neuroprosthetics.

Depending on their nature and severity, such changes could negatively impact hosts' **autonomy** and the **rejectability**, **integrity**, **utility**, **availability**, **authenticity**, and **distinguishability** of information experienced by the hosts or users, as well as potentially leading hosts to involuntarily disclose information in a way that damages its **confidentiality** and the hosts' **possession** of it.

---

vantage of Bionic Ears and Eyes" (2012). Regarding the possibility of neuroprosthetic devices being used to provide false data or information to their hosts or users, see also McGee, "Bioelectronics and Implanted Devices" (2008), p. 221. See also Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

<sup>70</sup> See Ramirez et al., "Creating a False Memory in the Hippocampus" 2013.

<sup>71</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), pp. 215-16, and Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 125, 130.

On the other hand, it is also possible that the structural and behavioral changes occurring in a host's brain as the result of using an advanced neuroprosthetic might have salutary effects that increase the host's **autonomy**, enhance the **integrity**, **availability**, and **utility** of information, and strengthen the host's ability to maintain the **confidentiality** and **possession** of that information. The designers of neuroprosthetic devices will need to conduct careful monitoring and testing to identify the short- and long-term effects of the devices' use and discover potentially unexpected side-effects that may have an impact on information security.

## The host as embodied embedded organism

### FUNCTIONAL CAPACITIES CREATED BY A NEUROPROSTHETIC DEVICE

Below we describe some of the new functional capacities that a neuroprosthetic device can provide its human host or user in his or her role as an embodied embedded organism and the potential impact that these capacities might have on the information security of the host-device system.<sup>72</sup>

#### *Sensory enhancement*

A neuroprosthetic device may allow its host or user to sense his or her physical or virtual environment in new ways, either by acquiring new kinds of raw sense data or new modes or abilities for processing, manipulating, and interpreting sense data.<sup>73</sup>

The **availability**, **integrity**, **utility**, and **authenticity** of information provided by such devices depends not only on their quality and technical specifications but also on securing the devices from external manipulation. If the sense data that is being gathered by the devices and transmitted to the user's mind can be intercepted by external agents, the **confidentiality** and **possession** of that information is undermined. Such devices also raise questions of **rejectability** if the user cannot block out the information that they provide. The extent to which information provided by the neuroprosthetic device displays **distinctibility** from the user's other natural sensory input may depend not only on the device's technical capacities and limitations but also on explicit design decisions made by the device's producer about the ways in which information should be presented. Insofar as such devices might expand the capacities of their users to consciously experience sense data and make decisions on the

<sup>72</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>73</sup> See Warwick, "The cyborg revolution" (2014), p. 267; McGee, "Bioelectronics and Implanted Devices" (2008), p. 214; and Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 120, 126.

basis of it, such devices could potentially enhance their users' agency and **autonomy**.

#### ***Motor enhancement***

A neuroprosthetic device may give its host or user new ways of manipulating physical or virtual environments through his or her body.<sup>74</sup> For example, it might grant enhanced control over one's existing biological body, expand one's body to incorporate new devices (such as an exoskeleton or vehicle) through body schema engineering,<sup>75</sup> or allow the user to control external networked physical systems such as drones or 3D printers or virtual systems or phenomena within an immersive cyberworld.

Insofar as such mechanisms for motor enhancement provide proprioceptive or other sensory feedback, they would be subject to the issues noted above for neuroprosthetics that provide sensory enhancement. Neuroprosthetics that provide strengthened control over a host's body could enhance the **confidentiality** and **possession** of information by their hosts by preventing the inadvertent disclosure of information through motor actions such as speech or facial expressions. On the other hand, by extending or altering the host or user's body, such a device might simply create new motor avenues through which such information can be inadvertently disclosed.

#### ***Enhanced memory, skills, and knowledge accessible through sensory organs (exograms)***

A neuroprosthetic device may give its user access to external data-storage sites whose contents can be "played back" to the user's conscious awareness through his or her sensory organs or to real-time streams of sense data that augment or replace one's natural sense data.<sup>76</sup> The ability to record and play back one's own sense data could provide perfect audiovisual memory of one's experiences.<sup>77</sup>

Neuroprosthetics that store memories, skills, and other information as exograms<sup>78</sup> that are external to the brain's own natural mnemonic systems face

---

<sup>74</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), p. 213, and Warwick, "The cyborg revolution" (2014), p. 266.

<sup>75</sup> See Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics..." (2015).

<sup>76</sup> See Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 115, 120, 126.

<sup>77</sup> See Merkel et al., "Central Neural Prostheses" (2007); Robinett, "The consequences of fully understanding the brain" (2002); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>78</sup> E.g., devices of the sort described by Werkhoven, "Experience Machines: Capturing and Retrieving Personal Content" (2005), but in implantable rather than external wearable form.

different information security issues from those that store information in the form of engrams within the brain's natural mnemonic mechanisms. Information stored within engrams can be recalled by the user's mind without first needing to pass through sensory organs; the information appears to come "from within" the user's own mind, rather than being presented to the user's conscious awareness through the use of sensory organs as if the information were originating from some environment outside of the user's mind. The fact that the use of engrams bypasses the brain's sensory systems creates different information security capacities and concerns than the use of exograms that must be presented through sensory organs or sense modalities.

Because information stored as exograms can potentially take the form of conventional text, video, audio, or image files (rather than being stored as patterns of interconnection, activation functions, and learning processes within a neural network), it may be easier for unauthorized parties to access, manipulate, delete, or replace that information. On the other hand, the ability to store information in conventional file formats may allow the use of encryption and other security or access controls that are not possible for information stored as engrams within the brain's own neural networks – since information stored within the brain's own mnemonic systems must utilize whatever form and structure the brain is designed to handle rather than whatever more "secure" structures a security-conscious neuroprosthetic engineer might wish to impose.

Information stored in the form of exograms accessible through sensory systems would be subject to many of the same issues surrounding **integrity**, **utility**, **availability**, **confidentiality**, **authenticity**, and **possession** that currently apply, for example, to information that a user might store on a mobile device and access through earphones or a virtual reality headset. If a neuroprosthetic device can be used to forcibly present information or activate the use of skills against the user's will, then questions of **autonomy** and **rejectability** also arise.

#### **FUNCTIONAL IMPAIRMENTS CREATED BY A NEUROPROSTHETIC DEVICE**

Below we describe some of the functional impairments that a neuroprosthetic device might create for its host at the level of his or her physical or virtual bodily interfaces with the environments and the impact that these impairments might have on the information security of the host-device system.<sup>79</sup>

##### ***Loss of control over sensory organs***

A neuroprosthetic may deny its host or user direct control over his or her sensory organs.<sup>80</sup> Technologically mediated sensory systems may be subject

---

<sup>79</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>80</sup> Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage



to noise, malfunctions, and manipulation or forced sensory deprivation or overload occurring at the hands of sense hackers.<sup>81</sup>

A neuroprosthetic device that intentionally deprives its host or user of control over his or her sensory organs raises questions of the **rejectability** of sense data and may impair the host or user's exercise of agency and thus his or her **autonomy**. The **availability**, **integrity**, **utility**, and **authenticity** of information provided by the host or user's sensory organs will depend on the technical capacities and motives of whatever external agents control the design or operation of the neuroprosthetic device.

#### ***Loss of control over motor organs***

A neuroprosthetic device may impede its host or user's control over his or her motor organs.<sup>82</sup> The host or user's body may no longer be capable, e.g., of speech or movement, or the control over one's speech or movements may be assumed by some external agency.

A neuroprosthetic device that intentionally deprives its host or user of control over his or her motor organs may prevent that person from inadvertently (or even purposefully) disclosing information through the use of speech, facial expressions, typing, or other physical means, thereby enhancing the **confidentiality** and **possession** of information.

The use of such a device may impair the information security of outside parties who, for example, interact with the host in conversation, listen to the host giving a lecture, or read a message that was typed and sent by the host: such individuals might assume that the information was conveyed to them intentionally by the host, while in fact it might have been conveyed against the host's will by some external agent who was controlling the host's motor activity through the neuroprosthetic device. This would result in a loss of **authenticity** of the information shared by the "host," from the perspective of those who received it.

#### ***Loss of control over other bodily systems***

A neuroprosthetic device may impact the functioning of internal bodily processes such as respiration, cardiac activity, digestion, hormonal activity,

---

of Bionic Ears and Eyes" (2012), p. 130.

<sup>81</sup> Hansen and Hansen discuss the hypothetical case of a poorly designed prosthetic eye whose internal computer can be disabled if the eye is presented with a particular pattern of flashing lights. See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

<sup>82</sup> Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 216.

and other processes that are already affected by existing implantable medical devices.<sup>83</sup>

Insofar as a neuroprosthetic device interfaces directly with such biological systems and processes, it may gather, store, utilize, and transmit data about them that must be secured in order to avoid a loss of **confidentiality** and **possession** of the information. By affecting the body's basic biological processes, a device may impact the brain's ability to receive, generate, store, transmit, and consciously experience information and may thus indirectly affect the **availability** and **utility** of information available to the host or user's mind.

#### *Other biological side-effects*

A neuroprosthetic device may be constructed from components that are toxic or deteriorate in the body,<sup>84</sup> may be rejected by its host, or may be subject to mechanical, electronic, or software failures that harm their host's organism.

Depending on the nature and severity of such effects, negative impacts could result for a host's **autonomy** and the **rejectability**, **integrity**, **utility**, **availability**, **authenticity**, and **distinguishability** of information experienced by a host or user.

On the other hand, if an advanced neuroprosthetic device is only able to function for a limited period of time before its connection to the neural circuitry of its host breaks down and the device ceases to function, this behavior could function as a sort of safeguard that limits the long-term possibilities for the device to contribute to a loss of the **confidentiality** or **possession** of information.

## The host as social and economic actor

### **FUNCTIONAL CAPACITIES CREATED BY A NEUROPROSTHETIC DEVICE**

Below we describe some of the new functional capacities that a neuroprosthetic device might provide to allow its host or user to connect to, participate in, contribute to, and be influenced by social relationships and structures and networks of economic exchange, and we note the potential impact that these capacities might have on the information security of the host-device system.<sup>85</sup>

---

<sup>83</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), p. 209, and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), pp. 12-16.

<sup>84</sup> McGee, "Bioelectronics and Implanted Devices" (2008), pp. 213-16.

<sup>85</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

***Ability to participate in new kinds of social relations***

A neuroprosthetic device may grant its host or user the ability to participate in new kinds of technologically mediated social relations and structures that were previously impossible, perhaps including new forms of merged agency<sup>86</sup> or cybernetic networks that display utopian (or dystopian) characteristics that are not possible for non-neuroprosthetically-enabled societies.<sup>87</sup>

The creation of new kinds of social relationships may create new avenues for a host or user to inadvertently disclose information, thereby damaging its **confidentiality** and his or her **possession** of it. It may also provide new means for external agents to disrupt or influence the host or user's acquisition and use of information, not through manipulation of the device's components or systems but by using the device in its intended fashion to interact socially with its user and undermining the user's information security use through the nature and contents of those social interactions (which might involve social engineering<sup>88</sup>). This could indirectly impact the **availability** and **utility** of information for the user and may also potentially undermine his or her agency and thus **autonomy**.

***Ability to share collective knowledge, skills, and wisdom***

Neuroprosthetics may link hosts or users in a way that forms communication and information systems<sup>89</sup> that can generate greater collective knowledge, skills, and wisdom than are possessed by any individual member of the system.<sup>90</sup>

On the one hand, using a neuroprosthetic device to store information in communal systems that make their contents freely accessible to other human minds clearly eliminates the user's ability to maintain the **confidentiality** and

---

<sup>86</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), p. 216, and Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 125, 132.

<sup>87</sup> See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

<sup>88</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), pp. 307-23; Sasse et al., "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security" (2001); and Thonnard, "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat" (2012).

<sup>89</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), p. 214; Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 128-29; Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), p. 24; and Gladden, "Upgrading the Human Entity..." (2015).

<sup>90</sup> See Wiener, *Cybernetics* (1961), loc. 307off., 3149ff., and Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

**possession** of that information. On the other hand, by drawing information from “open-source” repositories whose maintenance and editing are crowdsourced to myriad minds that are continuously identifying and rectifying errors and which provide checks and balances to counteract one another’s biases, it may be possible for such “neuroprosthethically enabled wikis” to maintain a self-healing and self-correcting state that offers greater **availability**, **integrity**, and **utility** of information than that possible from a static source developed by a single author.

#### *Enhanced job flexibility and instant retraining*

By facilitating the creation, alteration, and deletion of information stored in engrams or exograms, a neuroprosthetic device may allow its user to download new knowledge or skills or instantly establish relationships for use in a new job.<sup>91</sup>

A neuroprosthetic device that allows its user to enhance his or her socioeconomic position by continuously improving his or her skills, enhancing his or her job performance, and moving into ever more desirable and rewarding professions and positions may provide the user with resources (including financial, informational, and human resources and access to new technologies embodied in hardware, software, and services) that allow him or her to enhance and strengthen his or her information security, including his or her **autonomy**, the **confidentiality** and **possession** of information already in his or her control, the **availability** of new kinds of information, and enhanced tools for extracting **utility** from information.

#### *Enhanced ability to manage complex technological systems*

By providing a direct interface to external computers and mediating its user’s interaction with them,<sup>92</sup> a neuroprosthetic device may grant an enhanced ability to manage complex technological systems that can be used, for example, for the production or provisioning of goods or services or the management of digital ecosystems and environments that utilize ubiquitous computing and are integrated into the Internet of Things.<sup>93</sup>

By giving the user of a neuroprosthetic device enhanced capacities for acquiring and managing information and controlling his or her environment, the device may offer the user increased **availability**, **utility**, **confidentiality**, **possession**, and **rejectability** of information.

---

<sup>91</sup> See Koops & Leenes, “Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes” (2012), p. 126, and Gladden, “Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems” (2015).

<sup>92</sup> McGee, “Bioelectronics and Implanted Devices” (2008), p. 210.

<sup>93</sup> See McGee, “Bioelectronics and Implanted Devices” (2008), pp. 214–15, and Gladden, “Cyber-shells, Shapeshifting, and Neuroprosthetics...” (2015).

***Enhanced personal and professional decision-making***

By analyzing data, offering recommendations, and alerting the user to potential cognitive biases, a neuroprosthetic device may enhance its user's ability to execute rapid and effective personal and professional decision-making and transactions.<sup>94</sup>

By enhancing its user's ability to avoid the effects of internal biases and to identify and counteract intentional or inadvertent efforts by others to manipulate the user through social interaction, such a neuroprosthetic device may enhance its user's agency and **autonomy** and help prevent the user from inadvertently making decisions or undertaking actions that would undermine the **confidentiality** or **possession** of the user's information. It may also lead the user to make decisions which will eventually put the user in a position in which he or she enjoys greater **availability** and **utility** of information.

***Store of monetary value***

By storing cryptocurrency keys within its internal memory, a neuroprosthetic may allow its host to house digital money directly within his or her brain that can be spent on demand by the host.<sup>95</sup>

The use of a neuroprosthetic device to store information that has direct monetary value – rather than simply confidential personal or professional information which an unauthorized party might steal and attempt to convert into money through its sale or through blackmail of the host – creates an enticing new target for criminals and a new kind of information that must be carefully secured. For many users, the **possession** and **confidentiality** of such financial information would take priority and must be safeguarded, even if it means reducing the **availability** and **utility** of the information to the user.

A neuroprosthetic device that can be used directly to purchase goods and services and engage in other forms of economic exchange may give its user new tools for acquiring, utilizing, and securing information, thereby increasing the **availability** and **utility** of information as well as its **confidentiality** and **possession**.

---

<sup>94</sup> Kooops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), p. 119.

<sup>95</sup> See Gladden, "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values" (2015).

*Qualifications for specific professions and roles*

Neuroprosthetics may provide persons with abilities that enhance job performance in particular fields<sup>96</sup> such as computer programming, art, architecture, music, economics, medicine, information science, e-sports, information security, law enforcement, and the military. This may initially provide a competitive advantage to individuals using certain kinds of neuroprosthetic devices, while not excluding from such work those who lack neuroprosthetic devices. However, it is expected that as the use of elective neuroprosthetics becomes more commonplace and employers' expectations for employees' neural integration into digital workplace systems grow, possession of neuroprosthetics may become a basic requirement for employment in some professions that excludes from consideration potential workers who do not possess such devices.<sup>97</sup>

Insofar as individuals' use of advanced neuroprosthetic devices is a necessary and important aspect of their professional work, it can be expected that such employees' workplaces and employers will create and maintain robust institutional support systems for the users of such devices, which may include the attention of information security professionals dedicated to securing the information contained in these device-host systems. Such support structures may provide employees with stronger mechanisms for ensuring the **availability, utility, integrity, confidentiality, and possession** of information than they could obtain on their own if they acquired and utilized their neuroprosthetic devices solely in a role as ordinary consumers and personal, non-institutional users of such devices.

On the other hand, by allowing their employers to exercise at least some of the responsibility for maintaining, managing, and securing their neuroprosthetic devices, such users might instead find that an employer claims and acquires access to a user's personal information that is produced or accessible through the neuroprosthetic device, thereby reducing the **confidentiality** and **possession** of information by the user and potentially raising questions for the user about the extent to which the information's **availability, integrity, and authenticity** can be relied upon.

**FUNCTIONAL IMPAIRMENTS CREATED BY A NEUROPROSTHETIC DEVICE**

Below we describe some of the functional impairments that a neuroprosthetic device might create for its host or user at the level of his or her social

---

<sup>96</sup> Kooops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 131-32.

<sup>97</sup> McGee, "Bioelectronics and Implanted Devices" (2008), pp. 211, 214-15; Warwick, "The cyborg revolution" (2014), p. 269.

and economic relationships and activity and the impact that these impairments might have on the information security of the host-device system.<sup>98</sup>

*Loss of ownership of one's body and intellectual property*

A neuroprosthetic device that is being leased by its human host rather than having been purchased would not belong to the host. Moreover, even a neuroprosthetic device that has been purchased by its host could potentially be subject to seizure by an outside party in some circumstances (e.g., after a declaration of bankruptcy by the host). Depending on the leasing or licensing terms, intellectual property produced by a neuroprosthetic device's host or user (including thoughts, memories, or speech) may be partly or wholly owned by the device's manufacturer or provider.<sup>99</sup>

This may result in binding limits on the **confidentiality**, **possession**, **availability**, and **utility** of information that can be enforced by the device's manufacturer or provider through either legal or technical means. The manufacturer or provider may also have the legal right and technical ability to forcibly present to the user's conscious or subconscious awareness explicit advertisements, product placements edited into the user's sense data, or other commercial information that undermines the **rejectability** and perhaps **distinguishability** and **authenticity** of information received through the device. The fine print of the leasing, licensing, or even purchase agreement may also specify that the device's manufacturer or provider has the legal right to utilize the device to gather on an ongoing basis information about its host or user (including information about his or her biological and mental processes), which the company can either use internally for its own purposes or perhaps rent or sell to other companies for their own uses. This would have the effect of significantly reducing the **confidentiality** and **possession** of personal information by the host or user.

On the other hand, by maintaining an ongoing financial relationship with the device's manufacturer or provider, the user may be able to make use of physical maintenance services, software updates and upgrades (including regular updating of antivirus and other security software), and other services provided by that firm which enhances the **confidentiality**, **possession**, **availability**, **utility**, and **integrity** of information experienced through the device.

---

<sup>98</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>99</sup> See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

*Creation of financial, technological, or social dependencies*

The host or user of a neuroprosthetic may no longer be able to function effectively without the device<sup>100</sup> and may become dependent on its manufacturer for hardware maintenance, software updates, and data security and on specialized medical care providers for diagnostics and treatment relating to the device.<sup>101</sup> A user may also require regular device upgrades in order to remain competitive in certain jobs for which the possession and expert use of such a device is a job requirement. High switching costs may make it impractical to shift to a competing producer's device after a host has installed an implant and committed to its manufacturer's particular digital ecosystem.

If the host or user of a neuroprosthetic device is likely to suffer biological, psychological, financial, professional, or social damage without such ongoing specialized support from a company, this creates a power relation in which the host or user is in a position of dependency (or even subjugation) and in which he or she may be willing to accept an exploitative situation in which the **confidentiality** and **possession** of his or her information is compromised by the company, his or her autonomy is diminished, and the **availability**, **utility**, **integrity**, and **rejectability** of information is subject to the whims (likely driven by financial considerations) of the company.

*Subjugation of the host to manipulation by external agency*

Instead of merely impeding its host or user's ability to possess and exercise agency, a neuroprosthetic may subject its host to control by some external agency. This could occur, e.g., if the host's memories, emotions, or volitions were manipulated by means of the device<sup>102</sup> or if the host joined with other minds to create a new form of social entity that possesses some shared agency.<sup>103</sup>

---

<sup>100</sup> Kooops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), p. 125.

<sup>101</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), p. 213. Brain scarring is a significant problem with neuroprosthetic devices involving electrodes implanted in the brain, and the administration before, during, and after implantation surgery of immunosuppressive drugs that reduce the wound healing response has been found to reduce scarring and cortical edemas; see See Polikov et al., "Response of brain tissue to chronically implanted neural electrodes" (2005), for a discussion of such issues. The possibility that the host of an implanted advanced neuroprosthetic device might become dependent throughout the rest of his or her life on the device's manufacturer (or another commercial entity) for a regular supply of potentially expensive and proprietary immunosuppressive drugs or other specialized medications is a theme that has been explored by futurologists and the creators of science fiction works; for an analysis of a prime fictional depiction, see Maj, "Rational Technotopia vs. Corporational Dystopia in 'Deus Ex: Human Revolution' Gameworld" (2015).

<sup>102</sup> Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), pp. 15-16.

<sup>103</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), p. 216, and Gladden, "Upgrading'



Such a situation would impair the host's **autonomy** and could be exploited to undermine the **confidentiality** and **possession** of the host's information. Depending on the level of access to the host's information that is gained by the external agent, the **authenticity**, **integrity**, **availability**, and **utility** of the host's information could also be imperiled.

***Social exclusion and fragmentation and employment discrimination***

The use of particular kinds of neuroprosthetics that are considered by a particular society to be of a "suspicious" or "undesirable" nature and whose presence and operation is detectable to parties other than their host or user may result in the shunning or mistreatment of such hosts or users<sup>104</sup> by those who question or actively oppose the use of such devices.<sup>105</sup> Hosts or users of such neuroprosthetic devices may find themselves formally or informally excluded from certain kinds of organizations and social relationships, or they may simply avoid certain kinds of relationships and situations in order to spare themselves the embarrassment or discomfort that might result from such interactions. Possession of some kinds of neuroprosthetics may exclude their hosts from employment in roles where "natural," unmodified workers are considered desirable or even required (e.g., for liability or security reasons).

It is also expected that some kinds of advanced neuroprosthetics will so radically transform their users' channels for communicating and interacting socially that they will eventually lose the desire and even ability to communicate with human beings who do not possess the relevant sort of neuroprosthetics; in this way, humanity as it exists today may fragment into numerous mutually incomprehensible "posthumanities" that share a geographical home on this planet but whose societies and civilizations occupy disjoint psychological, cultural, and technological spaces that do not intersect or overlap.<sup>106</sup>

---

the Human Entity..." (2015).

<sup>104</sup> Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012), pp. 124-25.

<sup>105</sup> For example, anecdotal accounts have already been reported of physical harassment and exclusion from places of business of individuals wearing external sensory prosthetics designed to generate visual augmented reality. See Greenberg, "Cyborg Discrimination? Scientist Says McDonald's Staff Tried To Pull Off His Google-Glass-Like Eyepiece, Then Threw Him Out" (2012), and Dvorsky, "What may be the world's first cybernetic hate crime unfolds in French McDonald's" (2012).

<sup>106</sup> See McGee, "Bioelectronics and Implanted Devices" (2008), pp. 214-16; Warwick, "The cyborg revolution" (2014), p. 271; and Rubin, "What Is the Good of Transhumanism?" (2008).

Such a splintering and narrowing of societies may possibly weaken the solidarity with other human beings exhibited by users of some kinds of advanced neuroprosthetics.<sup>107</sup>

If the users of certain kinds of neuroprosthetics were, in essence, to withdraw from “normal” human society and develop new societies accessible only to those who share similar technological augmentation, interests, and philosophies, one side-effect of this growing distance and insulation from human society could be an increase in the **confidentiality** and **possession** of information by the users of such technologies, insofar as the ability of unaugmented humans to initiate some kinds of attacks (such as social engineering efforts) might be significantly curtailed. At the same time, the users of such neuroprosthetic devices might find that their voluntary or involuntary distancing from the rest of humanity separates them legally, politically, commercially, socially, or technologically from information security systems and mechanisms that are available to other human beings, thereby potentially putting at risk the **integrity**, **availability**, **confidentiality**, and **possession** of the users’ information.

#### ***Vulnerability to data theft, blackmail, and extortion***

A hacker, computer virus, or other agent may be able to steal data contained in a neuroprosthetic device or use the device to gather data (potentially including the contents of thoughts, memories, or sensory experiences)<sup>108</sup> that could be used for blackmail, extortion, corporate espionage, or terrorism targeted against the device’s host or user or other individuals or institutions. Such an attacker could either carry out a one-time theft of information or embed in the device software (or even hardware) that allows ongoing access and the ability to utilize the device’s features and components as an instrument for information-gathering and surveillance, regardless of whether they were designed to be employable for such purposes.

The minds, personalities, interests, motivations, and values of all human beings are different, which means that the authors of certain kinds of social engineering attacks on high-value targets must take the time to learn about the subject of their intended operation and develop a customized plan of attack, and it cannot be known for certain in advance of the attack whether or not it will succeed and what unexpected obstacles might arise during its attempted execution.<sup>109</sup> If the target of such an attack possesses an advanced

<sup>107</sup> Koops & Leenes, “Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes” (2012), p. 127.

<sup>108</sup> See McGee, “Bioelectronics and Implanted Devices” (2008), p. 217; Koops & Leenes, “Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes” (2012), pp. 117, 130; and Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012), p. 21.

<sup>109</sup> See Rao & Nayak, *The InfoSec Handbook* (2014), pp. 307–23, and Sasse et al., “Transforming

neuroprosthetic device, this may give the attacker a means of planning and executing the attack that depends solely on technical and technological factors (which it may be possible to analyze carefully in advance) rather than social and psychological ones. Exploitable vulnerabilities in a particular model of neuroprosthetic device that have been identified by would-be attackers may place at risk all human beings who possess that particular model of device, regardless of the otherwise great psychological, cultural, and professional dissimilarities between them.

Depending on the exact purpose and nature of such an attack, it may have the potential to undermine the **confidentiality** and **possession** both of the host or user's information and the information of other parties that can be compromised by means of the neuroprosthetic device (e.g., by using a neuroprosthetic device implanted in one person to eavesdrop on a separate individual who happens to be nearby). It may also compromise the **authenticity**, **integrity**, **availability**, **distinguishability**, and **utility** of information and be employed to undermine the host or user's **autonomy**.

## Conclusion

In this chapter we have explored a two-dimensional conceptual framework for cognitional security that comprises nine essential information security goals for neuroprosthetic devices and device-host systems (confidentiality, integrity, availability, possession, authenticity, utility, distinguishability, rejectability, and autonomy) and examines potential impacts on the pursuit of those goals as observed at three different levels (which consider a device's host understood as sapient metavolitional agent, embodied embedded organism, and social and economic actor). In the following chapters we will draw on this cognitional security framework to consider important practical issues relating to the development and implementation of information security plans for advanced neuroprosthetics – namely, the formulation of particular information security roles and responsibilities and the design and use of management, operational, and technical controls.

---

the 'weakest link'—a human/computer interaction approach to usable and effective security" (2001).

## Part III

# **Security Practices and Mechanisms for Advanced Neuroprosthetics**



## Chapter Six

# Responsibility for Security Planning and Implementation

### Overview of security activities

The process of ensuring information security for a neuroprosthetic system involves the combined effort of many individuals carrying out different activities at many levels, regardless of whether the system is being used within a large institutional setting or by a single consumer. Here we consider classic descriptions of key information security roles and responsibilities and explore the ways in which these roles may need to be adjusted or complemented by newly defined roles and responsibilities that are uniquely important for an advanced neuroprosthetic system.

Information security roles and responsibilities relate to the execution of particular activities; it is thus useful to describe those activities before considering the individuals who will carry them out. The many activities needed to ensure information security can be organized according to their place within the system development life cycle (SDLC), which spans the period from when the first idea is raised about acquiring or developing a new system through the time when that system, no longer “new,” is eventually removed from service.<sup>1</sup>

In principle, a system development life cycle can be quite brief; it may only last days, weeks, or months, if the new system is small in scope and complexity and is being adopted only for a limited time to fulfill some *ad hoc* purpose. Although the key elements of the SDLC should still be present, in such a case they might appear in only a brief and simplified form.

In the case of an advanced neuroprosthetic device, the costs, risks, and complexity involved with implanting such devices into and removing them from human hosts means that their SDLC – and in particular, the operations

---

<sup>1</sup> NIST SP 800-100 (2006), pp. 19-25.

and maintenance phase of the SDLC during which the device is functioning within its human host – may be more likely to span years or even decades.

Below we consider the five main phases of the SDLC – the initiation, development and acquisition, implementation, operations and maintenance, and disposal phases – as they relate to advanced neuroprosthetics. Here we draw extensively on the more general description of these phases can be found in Chapter 3 of *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers*, produced by the National Institute of Standards & Technology. We have integrated into that general framework a number of other more detailed activities (such as awareness and training and the interconnection of systems) that are discussed elsewhere in *NIST SP800-100* but not explicitly as components of the SDLC.

## Initiation phase

### DETERMINATION OF NEEDS

During the initiation phase, the needs that should be filled by the neuroprosthetic device are specified.<sup>2</sup> For example, the device may be intended to function therapeutically in treating a particular medical condition or it may be designed to augment the abilities of a human user by providing some physical or psychological enhancement.<sup>3</sup> The required capacities and features that the device should possess are described at a general level.<sup>4</sup>

### SECURITY CATEGORIZATION

Next the kinds of information that the device will receive, generate, store, and transmit are identified. The relevant types of information can then be categorized using schemes such as those found in *NIST SP 800-60* and *FIPS 199*, thereby describing the nature and sensitivity of the information that the device will possess.<sup>5</sup> Knowing the kinds of information that the device will handle and the sensitivity of that information is essential in order to make effective decisions regarding the information security policies, practices, and mechanisms that will be employed. For example, a neuroprosthetic device that can access and record the contents of its host's mental processes or which can be used as a surveillance device to record nearby conversations will

---

<sup>2</sup> *NIST SP 800-100* (2006), p. 22.

<sup>3</sup> See Chapter One of this book for a discussion of different potential purposes for advanced neuroprosthetic devices and systems.

<sup>4</sup> *NIST SP 800-100* (2006), p. 22.

<sup>5</sup> *NIST SP 800-100* (2006), p. 22. See Chapter Four of this book for a device ontology that can be used to identify and classify such kinds of information.

require a much different information security plan than a neuroprosthetic device whose sole function is to stimulate the release of hormones within its user's body according to some regular schedule.

### **PRELIMINARY RISK ASSESSMENT**

A preliminary assessment is undertaken to “define the threat environment in which the system or product will operate.”<sup>6</sup> A neuroprosthetic device that will be used within a controlled clinical environment for medical research purposes and which cannot be modified by its user presents different risks than a mass-produced consumer neuroprosthetic device that will be used by individuals in their homes and workplaces and which can be modified by its users. A neuroprosthetic device for use by military personnel in battlefield operations – or cyberwarfare – will encounter still different risks.<sup>7</sup>

In the case of some kinds of neuroprosthetic devices, it may be difficult or impossible to specify a “typical” or “normal” operating environment, if that environment is influenced or determined by the cognitive processes of the host or user and the contents of his or her mental activity; in such a case, the operating environments presented by the minds of two different hosts could differ as greatly as do the memories, experiences, dreams, desires, and fears of two different people, and the operating environment presented by the mind of even a single host could change radically depending on the host's current emotional state and whether, for example, he or she is asleep or awake.

## **Development and acquisition phase**

### **REQUIREMENT ANALYSIS AND DEVELOPMENT**

Based on the decisions and information produced during the initiation phase, a more detailed analysis of requirements for the device (including information security requirements) is now carried out and specifications for the device are developed.<sup>8</sup>

### **RISK ASSESSMENT**

A more in-depth risk assessment is conducted, based on the device's specifications and intended (or possible) operating environments and informed

---

<sup>6</sup> *NIST SP 800-100* (2006), p. 22.

<sup>7</sup> On potential military use, see Schermer, “The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction” (2009), and Brunner & Schalk, “Brain-Computer Interaction” (2009).

<sup>8</sup> *NIST SP 800-100* (2006), p. 22. See Chapter Two of this text for a discussion of vulnerabilities of neuroprosthetic devices. For vulnerabilities in IMDs generally, see Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010).



by both functional, legal, and ethical considerations.<sup>9</sup> This process also includes the identification of vulnerabilities<sup>10</sup> and threats<sup>11</sup>, and the development of recommendations for security controls.<sup>12</sup>

### **COST CONSIDERATIONS AND REPORTING**

In many ways it would be easier to develop effective information security plans if cost were not an issue and unlimited financial and human resources could be dedicated to information security. In reality, the resources available to support information security are always limited and sometimes quite small relative to the scope, complexity, and importance of a project. InfoSec decision-makers often find themselves not developing the “best information security plan possible” but rather the “best information security plan possible given the resources available.”

Cost considerations must thus be carefully and realistically considered as part of the development and acquisition phase.<sup>13</sup> This is especially true for a neuroprosthetic device that may be permanently implanted in a human being, as analysis might indicate that the cost of ensuring information security for the device may be expected to increase or decrease significantly over the period of years or decades in which the device may be in use. Difficult and complex situations may arise, for example, if a neuroprosthetic device is implanted in a human being by the host’s employer and the information security costs are borne by the institution as long as the person is an employee, but financial and technical support ceases upon termination of the host’s employment.

### **SECURITY PLANNING**

A comprehensive device or system security plan (including documentation for all security controls<sup>14</sup>) is developed to guide the subsequent phases

---

<sup>9</sup> *NIST SP 800-100* (2006), p. 22. For an overview of ethical issues with ICT implants – many of which are relevant for advanced neuroprosthetics – see Hildebrandt & Anrig, “Ethical Implications of ICT Implants” (2012). For ethical issues in information security more generally, see Brey, “Ethical Aspects of Information Security and Privacy” (2007).

<sup>10</sup> *NIST SP 800-100* (2006), p. 88.

<sup>11</sup> *NIST SP 800-100* (2006), p. 87. For a discussion of threats to neuroprosthetic devices, see Chapter Two of this text and Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009). For threats to IMDs generally, see Halperin et al., “Security and privacy for implantable medical devices” (2008); for threats to BSNs, see Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012).

<sup>12</sup> *NIST SP 800-100* (2006), p. 90.

<sup>13</sup> *NIST SP 800-100* (2006), p. 90.

<sup>14</sup> For the importance of documentation especially for enterprise information systems, see Chaudhry et al., “Enterprise Information Systems Security: A Conceptual Framework” (2012).

and processes. Complementary resources such as training materials and manuals for administrators and users are also prepared.<sup>15</sup>

The system security plan does not simply address the information security performance of the implantable neuroprosthetic unit itself nor only when operating under nominal conditions. The plan should also incorporate information technology contingency planning for dealing with anomalous situations<sup>16</sup> and it should consider the information security performance of the joint systems that the neuroprosthetic unit will create through its integration and interconnection with other systems (including the outcomes that will occur, for example, if an emergency disconnection of the neuroprosthetic unit from its complementary systems must be performed<sup>17</sup>).

### SECURITY CONTROL DEVELOPMENT

The security controls described in the system security plan are now designed and implemented.<sup>18</sup> Note that insofar as possible, all security controls are implemented within the system before the system itself is implemented within the production environment in which it will operate; while it may be possible to implement all of the logical (and perhaps physical) controls prior to the system's deployment, it may only be possible to implement the full range of administrative controls after the system has been deployed and all of the relevant personnel and offices that will manage the use of the administrative controls are fully engaged with the use of the system.<sup>19</sup>

Particular kinds of security controls that may be relevant for advanced neuroprosthetic devices will be described in more detail in later sections of this book.

### DEVELOPMENTAL SECURITY TEST AND EVALUATION

Insofar as possible, all security controls are tested to determine their effectiveness prior to the system's deployment so that weaknesses and problems can be identified, changes and improvements can be made, and the sys-

---

Some advanced neuroprosthetic devices might indeed be used in such a context, as components of enterprise information systems.

<sup>15</sup> *NIST SP 800-100* (2006), pp. 23, 26-34.

<sup>16</sup> *NIST SP 800-100* (2006), pp. 78-82. See Chapter Three of this text for a discussion of the need to access neuroprosthetic devices during health emergencies experienced by their human host. See also Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012); Rotter & Gasson, "Implantable Medical Devices: Privacy and Security Concerns" (2012); and Halperin et al., "Security and privacy for implantable medical devices" (2008) – all of whom raise the issue of emergency access to IMDs. Halperin et al., especially, consider this question in detail.

<sup>17</sup> *NIST SP 800-100* (2006), p. 52.

<sup>18</sup> *NIST SP 800-100* (2006), pp. 23, 113-23.

<sup>19</sup> *NIST SP 800-100* (2006), p. 23.

tem can then be retested. Specific scenarios (such as hacking and social engineering attempts, the presence of computer viruses, operator error, and the failure of equipment or power supplies) may be prepared and their effects played out in order to evaluate the system's response.<sup>20</sup>

For some kinds of neuroprosthetic devices, it will not be possible to robustly test the system's information security features and performance until after the device has been implanted in its human host, insofar as the physical and cognitive connections between the device and host are among the key processes whose information security performance must be tested and the integration of the device into the host's biological systems and psychological processes cannot easily be simulated prior to the device's implantation.

#### **OTHER PLANNING COMPONENTS**

Other planning components that are carried out during the development and acquisition phase include considering the kinds of contracts<sup>21</sup> and agreements that will need to be developed between suppliers of raw materials, component and device manufacturers, software designers, distributors, implantation and medical support organizations, and end users.

### **Implementation phase**

#### **SECURITY TEST AND EVALUATION**

Final pre-deployment testing of the system's information security performance is undertaken in part to gather data about the system's baseline functioning and in part to ensure that the final set of security policies, practices, and mechanisms utilized by the system meets all relevant legal and regulatory requirements and satisfies ethical standards.<sup>22</sup>

In the case of an advanced neuroprosthetic device, legal, regulatory, and ethical issues surrounding the privacy of personal medical data will be a particular concern. Even if the device is being used by its host as an entertainment device or to enhance work productivity – and is not thought of primarily as a “medical device” – the system may still be interacting with the host's body

---

<sup>20</sup> NIST SP 800-100 (2006), p. 23.

<sup>21</sup> NIST SP 800-100 (2006), p. 23.

<sup>22</sup> NIST SP 800-100 (2006), p. 23. On the role of regulators and regulation, see McCullagh et al., “Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology” (2013); Patil & Turner, “The Development of Brain-Machine Interface Neuroprosthetic Devices” (2008); and Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants” (2012).

and gathering data in such a way that subjects it to potentially restrictive and intense legal and regulatory regimes.

The final pre-deployment testing of the system's information security performance should not test the system in isolation but, insofar as possible, should test the interaction of the system with all of the other systems with which it will be interconnected or on which it may be dependent.<sup>23</sup>

### **INSPECTION AND ACCEPTANCE**

The operator who is accepting the neuroprosthetic device for use verifies that all of the information security features and capacities that were required as part of the device's specifications are indeed present and functional in the finished product as supplied by the developer or manufacturer.<sup>24</sup>

### **SYSTEM INTEGRATION AND INSTALLATION**

The device is deployed as the necessary steps are taken to "Integrate the system at the operational site where it is to be deployed for operation" and to "Enable security control settings and switches in accordance with vendor instructions and proper security implementation guidance."<sup>25</sup>

In the case of many advanced neuroprosthetic devices, "system integration and installation" is constituted by the process of implanting the device into its human host, integrating the device with the host's neural circuitry, and activating the device.<sup>26</sup>

### **SECURITY CERTIFICATION**

Government agencies or large corporations may possess a "security certification" granted either by a senior official within the organization or by some external body certifying that the organization follows best practices for information security and that its systems utilize security controls, safeguards, and countermeasures that are sufficient to keep the organization's information secure.<sup>27</sup>

Existing certificates of this sort may need to be updated to include advanced neuroprosthetic systems newly adopted by the organization. For example, a government agency that has begun to employ personnel who possess artificial eyes that are capable of recording and transmitting live video would need to ensure that the addition of such devices to the workplace ecosystem

---

<sup>23</sup> NIST SP 800-100 (2006), p. 23.

<sup>24</sup> NIST SP 800-100 (2006), p. 23.

<sup>25</sup> NIST SP 800-100 (2006), p. 23.

<sup>26</sup> See Chapter One of this text for a general discussion of the integration of neuroprosthetic devices into the neural circuitry of their human host and Chapter Four for a device ontology that can be used to specify such interconnections for a particular device in more detail.

<sup>27</sup> NIST SP 800-100 (2006), p. 23.

does not compromise organizational information security. In the case of neuroprosthetic devices designed as consumer electronics products for use by individuals, the manufacturer may wish to reassure (potential) customers by obtaining certification from an independent body that – when used in accordance with the manufacturer’s instructions – the device will operate in a secure manner and will not compromise the user’s information security.

### **SECURITY ACCREDITATION**

Government agencies or large corporations whose personnel utilize neuroprosthetic devices may maintain a process of security accreditation by which a new kind of neuroprosthetic device is approved for use in receiving, generating, storing, or transmitting particular kinds of information.<sup>28</sup> Until a particular kind of neuroprosthetic device has received such accreditation, its hosts or users may be barred from accessing particular kinds of information or filling certain types of roles within the organization.<sup>29</sup>

Given the fact that the secure and effective functioning of an advanced neuroprosthetic device depends on the unique nature and extent of its integration with its human host and that the same type of neuroprosthetic device may operate very differently when implanted in different human hosts, some organizations may require a process of security accreditation not for each type of neuroprosthetic device, in general, but for each specific device-host pairing: the device as implanted and functioning in one human host may create a secure device-host system while in a different host the same type of device does not create such a system.

## **Operations and maintenance phase**

### **CONFIGURATION MANAGEMENT AND CONTROL**

A neuroprosthetic device may be capable of operating in many different configurations. The variation between configurations may arise from the installation of different software; the selection of different settings within the software; the addition, removal, or adjustment of hardware components; or the adjustment of the device’s relationship to and interconnection with its human host or external systems. In order to maximize information security, it is essential to choose the correct initial configuration for the device, change

---

<sup>28</sup> *NIST SP 800-100* (2006), p. 24.

<sup>29</sup> See Chapter Five of this text for a discussion of potential employment discrimination relating to advanced neuroprosthetic devices.

the configuration as needed, respond to environmental conditions or operational needs, and keep an accurate record of all changes to the configuration that have been made.<sup>30</sup>

For some kinds of neuroprosthetic devices, it may be difficult or impossible to clearly define different “configurations” that have been employed by the device. While many devices will include hardware or software settings that can be discretely adjusted and whose current configuration can be simply and precisely recorded, other neuroprosthetic devices might utilize, for example, electronic physical neural networks – or even living biological components – whose states are continually changing and evolving and are impossible to fully and precisely define.<sup>31</sup>

### CONTINUOUS MONITORING

After deployment of a neuroprosthetic device, continuous monitoring is required in order to determine whether the device’s actual operating conditions and environment are consistent with the conditions for which it was designed and to ensure that the security policies, practices, and mechanisms are functioning as intended.<sup>32</sup> Monitoring may include the automated generation and analysis of logfiles as well as manual audits and assessments that may be carried out with the use of particular software.<sup>33</sup>

The detection of anomalous conditions (whether a hardware failure or intentional attack on the system) may trigger an incident response including the deployment of countermeasures designed for “containment, eradication, and recovery” from the problem.<sup>34</sup> In the case of advanced neuroprosthetics, the kinds of countermeasures that can be employed will be constrained by legal, regulatory, and ethical considerations which place an obligation on the device’s operators to immediately and effectively address any incident that affects a device implanted within a human being – while simultaneously requiring that the health, safety, and well-being of the device’s human host not be compromised by any information security countermeasures utilized to respond to the incident affecting the device. (Such considerations would also apply when deploying countermeasures that are designed to directly affect the functioning of a system that is the source of an attack, if such a system itself may potentially be a neuroprosthetic device that is part of a device-host system with a human being and that person’s biological or psychological

---

<sup>30</sup> *NIST SP 800-100* (2006), p. 24.

<sup>31</sup> See the device ontology presented in Chapter Four of this text for a discussion of such physical neural networks.

<sup>32</sup> *NIST SP 800-100* (2006), p. 24.

<sup>33</sup> *NIST SP 800-100* (2006), p. 24.

<sup>34</sup> *NIST SP 800-100* (2006), pp. 124-29.

functioning may be damaged or otherwise adversely affected by countermeasures enacted against the device.<sup>35</sup>)

## Disposal phase

### INFORMATION PRESERVATION

The long-term disposition of information that is received by, generated by, stored in, and transmitted from the device must be determined.<sup>36</sup> Some kinds of information may be regularly archived, either within an implanted neuroprosthetic device itself, within an external component of the system, or in some other external unit, facility, or system. Some information that is stored within a neuroprosthetic device may only be recoverable after the device is removed from its human host. For information that is encrypted, access to the cryptographic keys must be appropriately maintained.<sup>37</sup> If information is automatically archived, for example, wirelessly to some commercial cloud-based service, the information security performance of that system and its interaction with the device must be carefully considered and tested.<sup>38</sup>

Some information that is generated or received by the system on an ongoing basis (e.g., input generated by the host's biological processes) might in effect be "destroyed," simply because it is used instantaneously by the system and is not recorded in any format capable of being preserved. Other information that has been recorded may be subject to intentional destruction. Complex legal, regulatory, and ethical considerations may dictate that some kinds of information must be preserved and other kinds may not be, especially in light of the neuroprosthetic device's status as a medical device that may gather sensitive medical data about its user.<sup>39</sup>

---

<sup>35</sup> For a discussion of current legal and ethical issues involved, e.g., with the use of offensive countermeasures to mitigate a botnet, see Leder et al., "Proactive Botnet Countermeasures: An Offensive Approach" (2009).

<sup>36</sup> *NIST SP 800-100* (2006), p. 24.

<sup>37</sup> *NIST SP 800-100* (2006), p. 24.

<sup>38</sup> For information security issues specific to cloud-based systems, see Fernandes et al., "Security Issues in Cloud Environments: A Survey" (2013).

<sup>39</sup> Regarding regulatory and legal issues, see McCullagh et al., "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology" (2013); Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008); and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012).

### **MEDIA SANITIZATION**

The sanitizing of storage media may involve processes such as overwriting existing data with new data, degaussing a magnetic drive, or physically destroying the media.<sup>40</sup> For those components of a neuroprosthetic system that exist outside of the human host's body, the sanitization of media may not raise any special considerations. However, the sanitization of media that are contained within the host's body must generally be performed in a way that does not harm the host. In some cases, it may be difficult or impossible to verify that the information has been completely removed from the media without extracting the media from the host's body.

### **HARDWARE AND SOFTWARE DISPOSAL**

The disposal of neuroprosthetic hardware and software must be carried out in an appropriate manner in order to ensure information security.<sup>41</sup> The memory components of a used device may contain highly sensitive data about the biological and cognitive activity of its former human host. Moreover, the unit may be contaminated with biological matter that contains DNA from the host and other substances that could be analyzed to reveal information about the former host's health, activities, or environment.

## **Roles and responsibilities for information security**

The security activities described above are carried out by one or more *participants* in an advanced neuroprosthetic system who fill specific *roles* that give them particular *responsibilities* for executing or overseeing security activities.<sup>42</sup>

### **Individuals and organizations participating in an advanced neuroprosthetic system**

Typically, the production and use of an advanced neuroprosthetic system is a complex process that involves the participation of multiple individuals or organizations. Below we identify some of the common participants in that process and highlight ways in which they may contribute to the successful planning and execution of the information security activities described above.

#### **DEVICE DESIGNER**

The organization or individual that designs the physical device may or may not be responsible for manufacturing it; the company that has developed

---

<sup>40</sup> NIST SP 800-100 (2006), p. 24.

<sup>41</sup> NIST SP 800-100 (2006), p. 24.

<sup>42</sup> NIST SP 800-100 (2006), p. 68.



the specifications and schematics for a device may then hire other firms to manufacture the device's components and systems and even to perform final assembly. The device designer may or may not also create the operating system that will run on the device.<sup>43</sup>

### ***Information security responsibilities***

The designer of an advanced neuroprosthetic device plays the key role in determining those basic security controls that are built into the physical device at time of its manufacture; by determining the device's specifications and functionality, the designer also sets key physical and technological parameters which determine the kinds of security controls that can (or cannot) be implemented later by other parties and which determine the kinds of basic vulnerabilities, threats, and risks to which the device may be prone.

If a neuroprosthetic device is produced with some security controls built into it as part of its original design specifications, the device's designer will likely exercise responsibility for security activities within the SDLC including carrying out a **determination of needs, security categorization, preliminary risk assessment, requirement analysis and development, risk assessment, cost consideration and reporting, security planning, security control development, developmental security test and evaluation, and other planning components**, insofar as they relate to the development and testing of those built-in controls. Note that because the designer may not have a clear understanding of the end purposes for which a device's operators will utilize the device, the controls developed by the designer may be of a basic and generalized nature and may need to be supplemented (or replaced) by other controls developed by the operator.

---

<sup>43</sup> Given the extent to which consumer electronics devices such as traditional desktop and laptop computers and mobile devices are subject to aftermarket hardware and software modifications by their purchasers and end users (even to the extent of the jailbreaking or rooting of smartphones by power users), it is impossible for a device's designer or manufacturer to know in advance exactly how end users might use a product. (For that point, see Chadwick, "Therapy, Enhancement and Improvement" (2008).) It is likely that among power users of advanced neuroprosthetic devices, a phenomenon (and even subculture) of modifying devices in unintended, unexpected, and potentially even illegal or unethical ways might emerge, as users push the limits of what is safe and possible for purposes of further enhancement and self-exploration. The ultimate hackers may not be those who hack external systems but who – through the use of neuroprosthetic devices – hack their own brain and mind. Denning et al. consider the possibility that while some users of neuroprosthetic devices might modify their devices in unexpected and unapproved ways in order to "enhance their performance, increase their level of pain relief, or over-stimulate the reward centers in the brain," others might do so intentionally to cause themselves harm; see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

Once a device's design has been completed and manufacturing and installation of physical devices has begun, the designer's ability to physically modify the basic security controls built into the device may be limited or nonexistent.

### **OPERATING SYSTEM DEVELOPER**

The organization or individual that develops the OS installed on a particular neuroprosthetic device may not have been responsible for the design of the device itself. For example, it may be the case (as is true now for many mobile devices utilizing the Android or Windows operating systems) that an existing operating system produced by one software designer is available for use by multiple device manufacturers, and manufacturers design their devices specifically to run that OS. Alternatively, a neuroprosthetic device that was distributed by its manufacturer with one OS installed could have that OS replaced by a different operating system that is manually installed by the device's user. On the other hand, it may be the case (as is true now for mobile devices utilizing the iOS operating system) that a single organization has designed both the physical device and the operating system with which it is distributed).

#### ***Information security responsibilities***

The developer of an advanced neuroprosthetic device's operating system may incorporate some security controls directly into the OS. In this case, the OS developer will likely exercise responsibility for security activities within the SDLC including carrying out a **determination of needs, security categorization, preliminary risk assessment, requirement analysis and development, risk assessment, cost consideration and reporting, security planning, security control development, developmental security test and evaluation, and other planning components**, insofar as they relate to the development and testing of controls built into the OS.

By determining the basic framework and environment within which any other software or applications will run on the device, the developer of the OS sets key parameters that determine the kinds of security controls that can (or cannot) be implemented later by other parties and which determine the kinds of basic vulnerabilities, threats, and risks to which the device may be prone.

Because the developer of the OS may not have a clear understanding of the end purposes for which a device's operators will utilize the device, the controls developed by the OS developer may be of a basic and generalized nature and may need to be supplemented (or replaced) by other controls developed by the operator.

Once a device has been installed, it may or may not be possible for the developer of its OS to modify the basic security controls built into the operating system through software updates or upgrades. If the developer of an OS

has the ability to access devices in use, gather information from the devices, and modify the OS, then the developer of the operating system may also exercise responsibilities in areas such as **configuration management and control**, **continuous monitoring**, and **information preservation**.

## **MANUFACTURER**

When the word is used in a general sense without qualifications, it may be assumed that an organization that is described as the “manufacturer” of an advanced neuroprosthetic device has designed the physical device, designed or selected its operating system, physically produced the device by assembling its components, and installed the operating system. In a more specific sense, a “component manufacturer” can be understood as an organization that produces one or more components that are incorporated into a device and the “device manufacturer” can be understood as the organization that directs the process of assembling all components into a finished device. The manufacturer may also have designed the device, or it may have produced the device on behalf of its designer.

### *Information security responsibilities*

The manufacturer of an advanced neuroprosthetic device plays a key role in ensuring that the finished product that is ready for distribution, installation, and use possesses the security controls described in the design specifications for the device (and potentially also for its OS).

The manufacturer may exercise responsibility for security activities within the SDLC including carrying out **security control development**, **developmental security test and evaluation**, and **other planning components**, insofar as they relate to the development and testing of controls built into the device and its OS. The manufacturer may also have responsibility for **hardware and software disposal** for components and finished units that are produced but not distributed or which are returned by the devices’ users due to manufacturing defects, the termination of a leasing arrangement, or other circumstances.

## **PROVIDER**

A device’s provider is the organization that makes it available to the user for implantation and use. In some cases, the device’s manufacturer may be a company that directly sell or lease the device to users; in that case, the manufacturer is also a provider. In the case of an advanced neuroprosthetic device that is used for therapeutic purposes, a hospital, charitable organization, insurance company, or government agency may provide the device to the human host who is also the device’s user, either for a fee or free of charge. In the case of an advanced neuroprosthetic device that is implanted into soldiers for

military use, the military organization may retain ownership and control of the device and serve as its operator while it is implanted in its human host. In this situation, one military agency that has produced the device may have provided it to another military agency that serves as the end user; in the sense in which we use the word here, the device has been physically implanted in its human host but not “provided” to the soldier for his or her use, as he or she may or may not even realize that the device has been implanted.<sup>44</sup>

### ***Information security responsibilities***

The provider of an advanced neuroprosthetic device may or may not play specific roles in information security within the device’s SDLC. At a minimum, the provider will ensure adequate information security for devices from the time when they are received from the manufacturer to the time of their delivery to the operator for implantation in the host.

Some providers may acquire neuroprosthetic devices from manufacturers and add their own customized components, operating system, or software before delivering them to operators; in this case, a device’s provider may exercise responsibility for security activities within the SDLC for their customized system including carrying out a **determination of needs, security categorization, preliminary risk assessment, requirement analysis and development, risk assessment, cost consideration and reporting, security planning, security control development, developmental security test and evaluation, and other planning components**, insofar as they relate to modification of the device from its original factory-default condition. The provider may also have responsibility for **hardware and software disposal** for units that are received from the manufacturer but never delivered to operators or which are returned by the devices’ users due to manufacturing defects, the termination of a leasing arrangement, or other circumstances.

### **INSTALLER / IMPLANTER**

The installer physical integrates the neuroprosthetic device into the physical organism and neural circuitry of its human host and activates the device. For some advanced neuroprosthetic devices, this will involve surgical implantation that is performed in a specialized medical facility. In other cases, the human host may already have been surgically implanted with a prosthetic sock, port, or jack into which neuroprosthetic devices (potentially many different kinds of devices) can easily be inserted; in this situation, it may be pos-

---

<sup>44</sup> For the possibility that human hosts might unwittingly have been implanted, e.g., with RFID devices, see Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012).

sible for the installation of a particular neuroprosthetic device to be performed by the device's host or another individual without any special training and outside of a medical facility.

#### ***Information security responsibilities***

The installer who performs the implantation of an advanced neuroprosthetic device into its human host and activation of the device plays a key role in ensuring that the security controls built into the device and software are able to function successfully. Failure to implant the device correctly or to fully activate its relevant features may create vulnerabilities, threats, and risks that compromise the information security of its operator and user.

The installer of an advanced neuroprosthetic device may bear particular responsibility for security activities such as the final pre-implementation **security test and evaluation** of the particular unit to be implanted, **inspection and acceptance** of the unit to be implanted, **system integration and installation**, **security certification** of the particular unit implanted, **configuration management and control**, and **continuous monitoring**. If the installer also participates in the repair or removal of neuroprosthetic devices that have been implanted in a human host, he or she may also have responsibility for **information preservation**, **media sanitization**, and **hardware and software disposal**.

#### **APPLICATION DEVELOPER**

For some neuroprosthetic devices, the only software that the devices are capable of running is the operating system that is installed by the device's manufacturer; there may not even be any physical means of accessing the device's memory to install new software. For other neuroprosthetic devices, it may be possible to install particular applications on the device and to run that software – regardless of whether or not this possibility was foreseen and intended by the device's designer and manufacturer.

Application developers may include any parties from the device's designer and manufacturer to authorized providers of third-party applications to the device's operator or host who create their own customized apps<sup>45</sup> to hackers who create software which, once installed, allows them to analyze and control the device to cybercriminals who create computer viruses or malware that can infect the unit.

---

<sup>45</sup> For factors that might cause a device's host to (licitly or illicitly) alter the functionality of his or her own implanted device, see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010).

### *Information security responsibilities*

The developer of an application for advanced neuroprosthetic device plays a role in ensuring information security for devices on which that software is installed and run. Depending on the circumstances, the application developer may or may not even realize that his or her application will be run on neuroprosthetic devices; if the application is designed to run on a general-purpose operating system such as Windows or Android, then neuroprosthetic devices utilizing the relevant operating system may be able to run the application, regardless of whether this was envisioned by its designer.

Software developers may exercise responsibility for security activities within the SDLC relating to their applications, including carrying out a **determination of needs, security categorization, preliminary risk assessment, requirement analysis and development, risk assessment, cost consideration and reporting, security planning, security control development, developmental security test and evaluation**, and **other planning components**. If the software developers have an official relationship with the device's designer, OS developer, manufacturer, provider, or operator, the software developer may carry out security activities in close collaboration with those partners and with a high level of commitment. Some software developers (including individual programmers who are not affiliated with a large company) may not have the resources needed to conduct some of the security activities at a robust level.

After an application has been delivered to a device's operator for installation on the device, the application's developer may or may not subsequently have an opportunity to modify the software and its security controls through software updates or upgrades. If the developer of an application has the ability to access devices in use that have the app running or installed, gather information from the devices, and modify the app, then the developer of the application may also exercise responsibilities in areas such as **configuration management and control, continuous monitoring**, and **information preservation** – either for the developer's own internal purposes or at the specific request of the device's operator (e.g., if the software developer maintains a cloud-based platform that services their application).

### **APPLICATION PROVIDER**

In some cases, it may be possible for an advanced neuroprosthetic device's operator or host to acquire third-party software directly from its developer and to install it on the device without any involvement or oversight on the part of the device's designer, manufacturer, or provider. In other cases, the device's designer, manufacturer, or provider may maintain control over the software that can be installed on the device by creating administrative, logical, or physical controls which require all software to be selected and installed

using a proprietary mechanism (such as a cloud-based app store) that is controlled by that party.

### *Information security responsibilities*

The application provider for an advanced neuroprosthetic device plays an important role in ensuring information security for the device by controlling the kinds of applications that can be installed and run on the device. Some application providers may simply be automated systems that allow any third-party developer to upload applications into the app store for download by users without any particular scrutiny being undertaken of the software's functionality or information security characteristics. In other cases, the application provider may serve as the developer of all of the software that it makes available for installation, or it may scrutinize software submitted for approval by third-party developers by carrying out security activities such as **risk assessment** and **security planning** to determine the criteria that must be met by third-party applications, a **security test and evaluation** and **inspection and acceptance** prior to making the software available for use by the device's operators, **system integration and installation** not into the neuroprosthetic devices themselves but into the provider's distribution systems, potentially a process of **security certification** to reassure device operators, **configuration management and control** to ensure compatibility and interoperability with other installed software, **continuous monitoring** of general performance and information security controls, and potentially **media sanitization** and **hardware and software disposal** mechanisms that ensure information security upon the uninstallation of the software by a device's operator.

### **OPERATOR / USER**

The operator or user of an advanced neuroprosthetic device is the organization or individual who controls the device's functioning. This may or may not also be the device's human host or the primary beneficiary of its functioning.<sup>46</sup>

In the case of a neuroprosthetic device whose functioning is directly controlled by the thoughts of its human host, the host would also be the device's operator. In the case of an artificial eye that can record and transmit live video and which has been implanted into an agent by a government organization for military or intelligence-gathering purposes, specialized government personnel may maintain ongoing remote control over the device and direct its

---

<sup>46</sup> See Chapter Three of this text for a discussion of the distinction between a device's host and user.

functioning; in this case, they would be the device's operators, and the device's human host may or may not even realize the purposes for which the device is being employed. In some cases, the device's host may be able to control some aspects of a device's functioning while medical or technological specialists control other aspects; in those situations, both parties serve as users and operators of the device. In other cases, a device may have no mechanism for receiving instructions from its host or any other outside agent but is instead directed entirely by its own software or internal artificial intelligence; in such a case one could say that the device has no operator (or is its own operator).

### ***Information security responsibilities***

The operator of an advanced neuroprosthetic device plays a critical role in ensuring information security by exercising responsibilities for security activities such as carrying out a **determination of needs, security categorization, preliminary risk assessment, requirement analysis and development, risk assessment, cost considerations and reporting**, and **security planning** for the specific environment within which and purpose for which the device will be deployed, **security control development** to design controls that are relevant to the specific circumstances in which the device will be used and which supplement or replace those basic controls built into the device's physical components, OS, and applications, **developmental security test and evaluation, other planning components** (including preparing contracts and agreements with the provider, installer, and other organizations or individuals that may provide maintenance services, as well as with the device's human host), a final pre-deployment **security test and evaluation** of the system as initially configured, **inspection and acceptance** of the device as initially configured, **system integration and installation** of the device to integrate it with the host's neural circuitry (through physical implantation in the host's body or through other means), and potentially **security certification** and **security accreditation** for the device in its intended environment and use.

The operator will especially bear responsibility for security activities including **configuration management** and **control and continuous monitoring** of the device after its installation and activation. The operator may also play the lead role in in **information preservation** during and after the device's period of active use and **media sanitization** and **hardware and software disposal** upon completion of its service lifetime.

### **HUMAN HOST**

The host of an advanced neuroprosthetic device is the human being into whose neural circuitry the device has been integrated. In some cases (e.g., with some forms of motor neuroprosthetics), an advanced neuroprosthetic device could potentially operate externally to the host's body in a noninvasive



fashion,<sup>47</sup> although this raises questions of the extent to which the device has truly been “integrated into” the host’s neural circuitry.<sup>48</sup>

In this text it is presumed that neuroprosthetic devices that are fully integrated into their host’s neural circuitry typically involve implantation into the host’s biological organism. (In some cases this may involve a stable long-term interface, although models of future neuroprosthetic systems comprising, for example, swarms of nanorobots operating within the host’s brain have also been proposed.<sup>49</sup>) However, there may be situations in which an initial neuroprosthetic device has been installed which includes a standardized external socket, port, or jack through which supplementary components or even entirely separate neuroprosthetic devices or external systems can be installed; in those cases, new newly-installed devices become integrated with the host’s neural circuitry but without necessarily enjoying any direct interface with the host’s natural biological structures or processes. Instead, the new device interfaces directly with the existing neuroprosthetic device and, through it, indirectly with the host’s biological neural systems.

A neuroprosthetic device’s human host may have purchased or leased the device, may have received it as a therapeutic aid or personal gift, may have received it as a productivity tool or fringe benefit from an employer, or may potentially have created the device himself or herself. The device may be implanted either permanently or for a predetermined or indeterminate temporary period. The human host may or may not be able to directly control the device and may or may not even realize that the device has been implanted.

### ***Information security responsibilities***

The host of an advanced neuroprosthetic device may or may not play a particular role in carrying out security activities designed to ensure the information security. In some cases, the user may not even realize that the device has been implanted in his or her body or (e.g., in the case of a host who is in a coma) may not be able to intentionally undertake any actions in support of the system’s information security. In other cases, the device’s host may also be its operator and directly control its use.

In his or her role as the human host of an advanced neuroprosthetic device, a person may especially bear responsibility for participating in security

---

<sup>47</sup> See Panoulas et al., “Brain-Computer Interface (BCI): Types, Processing Perspectives and Applications” (2010); Lebedev, “Brain-Machine Interfaces: An Overview” (2014); Birbaumer & Hagen, “Restoration of Movement and Thought from Neuroelectric and Metabolic Brain Activity: Brain-Computer Interfaces (BCIs)” (2007); and Gerhardt & Tresco, “Sensor Technology” (2008).

<sup>48</sup> See Chapter One of this text for a discussion of such questions.

<sup>49</sup> See Al-Hudhud, “On Swarming Medical Nanorobots” (2012).

activities such as **inspection and acceptance** of the device, **system integration and installation** through implantation of the device and activation of its features, **security certification** of the implanted device, **configuration management and control**, **continuous monitoring**, and **hardware and software disposal** upon the conclusion of their service lifetime.

### INFORMATION SECURITY COLLABORATION AMONG PARTICIPANTS

In the context of a large institution such as a military agency, an organization can potentially ensure the coherence and effectiveness of information security efforts by unifying the roles of device designer, OS developer, manufacturer, provider, installer, application developer, application provider, and operator of an advanced neuroprosthetic device, while the device's human host may also belong to the organization.

On the other hand, in the case of a neuroprosthetic device intended for broad use as a consumer electronics product, the situation can be very different: collectively, there is still a need to provide information security for such devices, but the system responsible for ensuring that security may not be a single unified organization but rather a disjointed patchwork of organizations and individuals who have very different interests, motives, and capacities and who may not have any ongoing relationship with one another. One participant in the system may or may not be able to assume good will and competence on the part of all the other parties. This can create significant obstacles to the pursuit of information security.

### Typical formalization of roles and responsibilities in an institutional setting

Within a government agency or large corporation the personnel structure for information security generally has several levels. Though the roster of organizational roles be more complex,<sup>50</sup> such a structure often includes the key roles of **chief information officer** (CIO), **information system owner**, **information owner**, and **information system security officer** (ISSO).

At the most general level of policy are individuals like the CIO whose task is to ensure that information security efforts are consistent with the organization's broad strategic goals and priorities and to allocate resources among and set objectives for their staff. At the most concrete levels are expert personnel with particular specializations (such as ISSOs) who work daily to implement information security policies effectively for specific systems. Below we consider the responsibilities traditionally associated with these roles and

---

<sup>50</sup> For example, a government agency may also have a senior agency information security officer (SAISO) who serves as a liaison between the CIO and ISSOs. See *NIST SP 800-100* (2006), p. 70.

the ways in which they might relate to advanced neuroprosthetic systems used within their organization.

### **CHIEF INFORMATION OFFICER (CIO)**

The CIO is the senior individual responsible for developing and maintaining information system security throughout an organization.<sup>51</sup> He or she develops job descriptions for key information security positions and ensures that highly qualified individuals are recruited, successfully trained and integrated into the organization, and supported in their work. Depending on the size of the organization, the degree to which the CIO is personally involved with developing all of the organization's information security policies, practices, and mechanisms will vary, however he or she does bear ultimate responsibility for ensuring that such procedures are developed and successfully implemented.

The CIO collaborates with leaders of other departments within the organization to ensure that the information security priorities and activities are consistent with and support the fulfillment of the organization's legal and regulatory obligations, ethical aims, and strategic and financial objectives. Conversely, the CIO ensures that the expertise, insights, and objectives of personnel within the InfoSec office inform and shape, as appropriate, the overall strategic direction and decisions of the organization as well as the work of other individual departments.

With regard to ensuring information security for neuroprosthetic devices and systems, the CIO has potential responsibilities relating to at least four different spheres: 1) the use of neuroprosthetics by the organization's **customers and clients**; 2) the use of neuroprosthetics by the organization's **employees and personnel**; 3) the use of neuroprosthetics by the organization's **competitors**; and 4) the use of neuroprosthetics by **hackers, cybercriminals, and other outside parties** who may potentially be employed by the company's competitors as part of business intelligence or corporate espionage campaigns or who may have their own financial, political, or personal motives.

#### ***Responsibilities regarding neuroprosthetics used by the organization's customers and clients***

For a company that produces neuroprosthetic technologies, it would be individuals such as the chief technology officer (CTO) or chief marketing officer (CMO), and not the CIO, who is primarily responsible for envisioning

---

<sup>51</sup> NIST SP 800-100 (2006), p. 68.

and developing new products and ensuring that they will provide information security capacities and features that are satisfactory for end users.

If, however, the company provides ongoing monitoring and maintenance for its devices, maintains a centralized “app store” that allows users to acquire new software for their devices, provides cloud-based storage for use by the devices, or otherwise integrates the neuroprosthetic devices that it manufactures into the company’s technological systems after the devices are in use by consumers, the CIO would play the key role in ensuring the information security of such systems and arrangements.

Even for an organization that has no involvement with the production or distribution of neuroprosthetic devices, the organization’s CIO must be concerned with ways in which the use of neuroprosthetics by customers may impact the company’s information security. For example, some organizations that produce films, live theater, art exhibitions, concerts, or sporting events have developed (and attempt to enforce) policies that bar customers from videotaping the event and, in particular, from making any such unauthorized videos publically accessible (e.g., through a video streaming site). Such policies may become legally and ethically untenable (not to mention commercially unsound) if in the future sufficient numbers of human beings possess artificial eyes that continually record live video of everything that their hosts visually experience and the streaming and public sharing of such videos comes to be seen as a normal part of human existence – and potentially even a protected form of freedom of expression and the “fair use” of others’ intellectual property. In such a situation, questions regarding the protection of an organization’s proprietary information and intellectual property may involve complex legal and technological questions that a CIO would need to address.

***Responsibilities regarding neuroprosthetics used by the organization’s employees and personnel***

The use of advanced neuroprosthetics by an organization’s personnel may take one of two forms:

- **Neuroprosthetics personally acquired and owned by an organization’s personnel.** It is possible that individuals who happen to work in the organization may have acquired such devices on their own, for their own personal ends and using their own financial resources. In this case, the organization may not necessarily even know whether its personnel possess such devices – and may even be legally barred from attempting to discover whether they do, insofar as an individual’s status as someone who does or does not possess neuroprosthetic devices may be legally protected personal medical information, and making employment-related decisions on the basis of such information could, in some circumstances, be considered a form of illegal employment

discrimination. A CIO may thus need to ensure that his or her organization's security controls are robust enough to deal with the case, for example, of an employee who possesses an artificial eye and who (without any ill intentions on the employee's part, and perhaps even without the employee's knowledge) is recording everything that appears on the employee's computer screen – without the organization being able to know whether any of its personnel actually possess such devices.

At some point, the organization may choose to proactively take advantage of the fact that some of its personnel not only voluntarily *acknowledge* the fact that they have acquired neuroprosthetic devices but actively request that they be allowed to interconnect their devices with the organization's information systems in order to more effectively and efficiently carry out their work. Such a phenomenon would follow the pattern seen in recent decades with mobile devices and the gradual development of “bring your own device” (BYOD) policies in which organizations attempt to support the use of official organizational systems (such as email, CRM and HRM software, and countless other cloud-based systems) on the bewildering array of mobile devices that have been personally acquired by the organization's personnel.<sup>52</sup>

- **Neuroprosthetics provided by an organization to its personnel.** There may be situations in which an organization acquires neuroprosthetic devices that it implants in its personnel. In this case, the organization may – subject to relevant laws and employment agreements with its personnel – maintain ownership of the devices even after they are implanted and bear ultimate responsibility for the devices' information security, which may be fully and directly integrated into (and even controlled by) organizational information systems. Such a situation might occur, for example, with a military organization that provides its personnel with advanced neuroprosthetics intended for use in combat situations, intelligence-gathering, or other operations.

***Responsibilities regarding neuroprosthetics used by the organization's competitors***

If an organization's competitors are utilizing neuroprosthetic devices in order to work more effectively and efficiently, develop new products and services to offer to customers, and otherwise achieve competitive advantages, it

---

<sup>52</sup> See Armando et al., “Formal Modeling and Automatic Enforcement of Bring Your Own Device Policies” (2014), for a discussion of some issues relating to BYOD issues and proposed solutions

would likely be senior executives such as the organization's Chief Human Resources Officer (CHRO), CMO, or Chief Strategy Officer (CSO) – and not the CIO – who lead the debate about whether the organization should itself utilize advanced neuroprosthetics among its personnel in order to build or maintain a competitive advantage.

On the other hand, if an organization's competitors are employing advanced neuroprosthetic devices in an effort to conduct business intelligence operations against the organization or otherwise acquire sensitive or proprietary information that would be of use to the competitors in undermining the organization's competitive position or advancing their own interests, the organization's CIO would play a key role in ensuring that the organization's information security policies, practices, and mechanisms minimize competitors' ability to utilize neuroprosthetic devices to acquire such information. Competitors' efforts to acquire business intelligence about the organization may utilize legitimate and accepted techniques that are neither illegal nor unethical, and the extent to which an organization can attempt to block the gathering of such intelligence may be constrained by legal, ethical, and cultural factors. However, the CIO will attempt to ensure that – while respecting such constraints – the organization's information security is not compromised by competitors' use of neuroprosthetic devices to gather information.

***Responsibilities regarding neuroprosthetics used by hackers, cybercriminals, and other outside parties***

An organization's CIO takes the lead in protecting the organization's information against the dangers posed by individuals or organizations that are willing to employ potentially illegal or unethical means in order to gain unauthorized access to the organization's systems and information. Such efforts at gaining unauthorized access may sometimes be undertaken by hackers who are trying to break into a system simply in order to prove to themselves that it can be done and to discover how the system works, and who have no desire to otherwise harm the organization or financially exploit such access.<sup>53</sup> On the other hand, efforts at gaining unauthorized access to a system and its information may sometimes be made by cybercriminals who are intent on exploiting such access for purposes of blackmail, extortion, or otherwise harming the company (and potentially its individual employees and customers).

Insofar as advanced neuroprosthetic devices provide their users with enhanced sensory, cognitive, or motor capacities and allow them to interface with physical and virtual systems in ways that were previously impossible,

---

<sup>53</sup> For a discussion of hackers' motives and interests, see Zarod, "Constructing Hackers. Professional Biographies of Polish Hackers" (2015).

hackers and cybercriminals may develop techniques for utilizing such neuroprosthetics in ways that facilitate their ability to gain and maintain unauthorized access to systems and information.<sup>54</sup> The potential use of advanced neuroprosthetics by unauthorized parties to gain access to an organization's systems and information creates at least two issues that a CIO must consider:

- **The creation of new kinds of vulnerabilities, threats, and risks.** The use of such neuroprosthetics may create entirely new kinds of vulnerabilities, threats, and risks that did not previously exist and which the organization must address through its information security planning and procedures.
- **The risk of harming human beings through the application of information security countermeasures.** A CIO must take into account the fact that some kinds of proactive or offensive countermeasures that an organization can theoretically deploy against potential or actual attacks have the capacity to disrupt the performance, functioning, and, in principle, even structural components of the remote systems responsible for initiating and undertaking the attack. Complex legal and ethical questions already surround the use of proactive countermeasures to repel or disrupt cyberattacks (e.g., launching temporary denial of service attacks against command-and-control servers in an effort to mitigate botnets<sup>55</sup>), and these questions become even more complex – and potentially create new legal and moral responsibilities for an organization – if the remote computer that is launching a hacking attempt and which might be disrupted or damaged by the organization's countermeasures is not a conventional desktop computer or server but an advanced neuroprosthetic device implanted in the brain of a human being – who may be the hacker who is directing the attack or may simply be an innocent third party whose neural implant has been hijacked and, unbeknownst to the person, is being used to participate in the attack. In this case, disrupting the operations of that neuroprosthetic device or otherwise damaging it could result in significant temporary or permanent physical or psychological harm – potentially including even death – for the host in whom the device is implanted, if the device possesses interconnections with the host's biological and cognitive systems that make those systems dependent on the device's

---

<sup>54</sup> See Chapter Three of this text for a discussion of possible uses of neuroprosthetic devices as a means for carrying out such attacks.

<sup>55</sup> See Leder et al., "Proactive Botnet Countermeasures: An Offensive Approach" (2009).

correct functioning or subject to damage by its anomalous functioning. This raises complicated questions regarding legal, ethical, and financial liability on the part of an organization that deploys such countermeasures.

### INFORMATION SYSTEM OWNER

The information system owner is “responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system.”<sup>56</sup> This individual participates in the development of the system security plan, and upon implementation of the system he or she ensures that personnel using the system receive the relevant information security training and use the system in a way consistent with the system security plan.<sup>57</sup>

### INFORMATION OWNER

The information owner is the individual who has been given “authority for specified information and is responsible for establishing the controls for information generation, collection, processing, dissemination, and disposal.”<sup>58</sup> Based on his or her expert knowledge of the relevant legal, ethical, and operational considerations, the information owner determines which individuals or systems should have which levels of access to which kinds of information and the ways in which they should be allowed to use or manipulate the information. He or she works closely with the system’s designers and operators to ensure that the security controls developed and implemented for the system provide the appropriate levels of access to the relevant individuals or systems.

In the case of an advanced neuroprosthetic device, complex legal and regulatory regimes govern the ownership of information that is received, created, stored, or transmitted by the device.<sup>59</sup> Depending on the exact nature of the device, the kind of information that it handles, and the contracts and agreements that have been formed between the relevant parties, information may be owned by the human host in whom the device is implanted, the device’s manufacturer, the device’s operator, or unrelated outside parties. For example, a single neuroprosthetic device might contain data about the biological processes of its host that has been gathered by the device and which is considered personal medical data, proprietary operating system software

---

<sup>56</sup> NIST SP 800-100 (2006), p. 69.

<sup>57</sup> NIST SP 800-100 (2006), p. 69.

<sup>58</sup> NIST SP 800-100 (2006), p. 69.

<sup>59</sup> See Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants” (2012); McGee, “Bioelectronics and Implanted Devices” (2008); Mak, “Ethical Values for E-Society: Information, Security and Privacy” (2010); McGrath & Scanail, “Regulations and Standards: Considerations for Sensor Technologies” (2013); and Shoniregun et al., “Introduction to E-Healthcare Information Security” (2010).



that was created and installed by the firm that manufactured the device, proprietary application software that was created and installed by the host's employer that is operating the device, and third-party text, video, audio, or image files that have been downloaded from the Internet onto the device by its user or host.<sup>60</sup>

### **INFORMATION SYSTEM SECURITY OFFICER (ISSO)**

In contrast to the CIO, who has responsibility for all aspects of information security for the entire organization, an information system security officer (ISSO) focuses on ensuring information security for one or more particular systems within the organization. The ISSO's focus on information security for the system also contrasts with the role of the information system owner, who must manage a broader range of strategic, legal, financial, and operational aspects of the information system that may or may not directly relate to its information security. The ISSO's role also differs from that of the information owner, insofar as the information owner is concerned first and foremost with the information as such (rather than the system or systems that are currently used to make it accessible to users) and he or she may lack expertise in the technological and security aspects of the information system that the ISSO should possess. The ISSO participates in the development of the system security plan and implementation of security controls and coordinates the work of the relevant individuals to ensure that the system security plan and security controls are updated as needed to respond to any future changes that must be made to the information system for operational or other reasons.<sup>61</sup>

In the case of an advanced neuroprosthetic device, an ISSO would need to combine expertise in in the field of information security with knowledge of fields such as biology, psychology, medicine, and biomedical engineering.

### **Potential specialized roles for future neuroprosthetic systems**

An advanced neuroprosthetic system will typically include the kinds of participants described above, such as a device designer, manufacturer, operator, and human host; if the manufacturer and operator are large institutions, they may also include individuals who have been formally assigned roles such as those of chief information officer (CIO) or information system security officer (ISSO).

---

<sup>60</sup> See the device ontology in Chapter Four of this text for an overview of the different kinds of possible information.

<sup>61</sup> *NIST SP 800-100* (2006), p. 70.

Depending on the exact form, capacities, environmental context, and intended use that a particular neuroprosthetic system possesses, some of the individuals involved with developing, producing, maintaining, operating, and securing that system may possess specialized roles that are not relevant for other kinds of neuroprosthetic devices or information systems more broadly. Such roles may be formally assigned or informally adopted. Examples of such roles that may be relevant for certain kinds of future neuroprosthetic devices and whose successful performance has implications for the information security of the neuroprosthetic system in which the individuals filling these roles participate include:

- **Body schema engineer / body designer.** A body schema engineer participates in the development, production, installation, or operation of advanced neuroprosthetic systems that provide their user with the experience of possessing and utilizing a body that is (potentially radically) nonhuman.<sup>62</sup> This would occur, for example, if a human being uses a neuroprosthetic device that replaces the person's natural sensory input with sensory input which creates the experience of possessing a nonhuman body that is inhabiting and operating within some virtual environment. Such possibilities already exist, for example, through the use of virtual reality headsets and haptic feedback with first-person video games in which the player takes on the role of a nonhuman character.<sup>63</sup> Alternatively, the physical body of a human being (apart from the brain) could be replaced with an artificial cybernetic body that is nonhuman in its form and functioning.<sup>64</sup> A body schema engineer would ensure that the human being's mind was capable of adapting successfully to the new nonhuman body and the potentially radically different biocybernetic sensorimotor feedback loop that it creates.

Many unique issues relating to information security would result; for example, the human owner of a new nonhuman body might discover that particular kinds of thoughts or volitions which – in the person's human body – had created purely internal mental phenomena will in this new body create gestures, expressions, vocalizations, or other physical expressions that can be detected and interpreted by others in a way that conveys information that the user would like to keep confidential.

---

<sup>62</sup> See Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics" (2015).

<sup>63</sup> See Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics" (2015).

<sup>64</sup> See Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics" (2015).

- **Neuromnemonic engineer / mnemonic designer / memory hacker.**

Some kinds of advanced mnemoprosthetic devices may affect or participate in a human mind's processes of encoding, storing, or retrieving memories in a way that allows the intentional alteration, enhancement, or removal of existing memories or the creation of new memories. Such future technologies allowing for the editing of human memories would be built on experimental results that have already been achieved with the use of optogenetic neuromodulation systems for the editing of memories in mice.<sup>65</sup>

A neuromnemonic engineer would develop tools and techniques for creating particular kinds of mnemonic content or bringing about particular kinds of targeted changes in existing mnemonic content within the human host's memory systems, while a mnemonic designer would utilize those tools to fashion a particular memory or "remembered experience" for some specific purpose. Significant questions of information security arise, insofar as the application of neuromnemonic engineering tools and techniques could, if used improperly, inadvertently destroy the only copy of information existing within a person's mind, and it may in some circumstances even be used intentionally to destroy particular information.<sup>66</sup> Moreover, the use of mnemocybernetics technologies to affect a particular person's memories (or even a human being's awareness of the possibility that such technologies *may* have been used) may create uncertainty for that individual about whether the information stored in his or her memories is true or false and an inability to trust any of his or her apparent memories.<sup>67</sup> The use of such technologies may also provide a mnemonic designer with the ability to access, interpret, and create an external record of (and perhaps even potentially "export" in an automated fashion) memories stored within the human host's mind that he or she wishes to keep confidential.

The extent to which mnemocybernetics technologies and neuromnemonic engineering can someday be implemented successfully for hu-

---

<sup>65</sup> See Han et al., "Selective Erasure of a Fear Memory" (2009), and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).

<sup>66</sup> For the possibility that an adversary might use a compromised neuroprosthetic device in order to alter, disrupt, or manipulate the memories of its host, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

<sup>67</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

man beings is still unclear and will depend on the resolution to numerous outstanding questions in the field of neuroscience. For example, if the Holonomic Brain Theory<sup>68</sup> is correct, the ability to create, modify, or delete complex, content-rich memories through the manipulation of a small number of neurons may prove not simply practically difficult but theoretically impossible.

- **Sensory engineer / sense sculptor / sense hacker.** Even if the basic shape and structure of a human being's body is not altered by a neuroprosthetic device, the device may subtly or radically reshape the way in which the body is used to experience the external environment. For example, a human being who appears completely normal but who possesses relevant neuroprosthetic devices may be experiencing the world by seeing with infrared and telescopic vision, hearing ultrasonic phenomena, and experiencing other sense data generated by magnetic fields, airborne chemicals, or other substances or phenomena in the environment which normal human beings are unable to detect.<sup>69</sup> Moreover, it is theoretically possible for sense data acquired through particular sensory organs to be "remapped" or "rerouted" so that it is received by the brain and perceived and interpreted by the mind using nonstandard sensory modalities. For example, instead of hearing ultrasound, it might be possible to "see" it; it may also be possible to directly "see" the existence of magnetic fields or to "hear" the presence of certain chemicals in the atmosphere.<sup>70</sup> A sensory engineer would develop technologies to allow for the remapping of sense data and alteration and enhancement of sensory modalities, while a sense designer or "sense sculptor" would work to fine-tune a person's sensory modalities to create the capacity for unique sensory experiences that are artistically and aesthetically meaningful and potentially unique. Questions of information security arise in such work, insofar as sense data can potentially be altered or "enhanced" in such ways that it no longer conveys accurate or useful information about the external environment;<sup>71</sup> moreover the technologies used to effect such sensory enhancement may potentially create vulnerabilities that could allow

---

<sup>68</sup> See Longuet-Higgins, "Holographic Model of Temporal Recall" (1968); Pribram, "Prolegomenon for a Holonomic Brain Theory" (1990); and Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web..." (1999).

<sup>69</sup> See Warwick, "The cyborg revolution" (2014); Gasson et al., "Human ICT Implants: From Invasive to Pervasive" (2012); and Merkel et al., "Central Neural Prostheses" (2007).

<sup>70</sup> See Wiener, *Cybernetics* (1961), loc. 2784ff; Lebedev, "Brain-Machine Interfaces: An Overview" (2014), p. 106; and Warwick, "The cyborg revolution" (2014).

<sup>71</sup> See Chapter Five of this text for a discussion of authenticity in sensation.

unauthorized parties to access the host's sensory experiences by accessing the devices that present them to the host's mind.

### Multiple roles for a single individual?

A single individual may fill more than one role, either temporarily or permanently. However, whenever a single person fill multiple roles there is a danger the danger that the effectiveness of the security planning process may be undermined: having each role filled by a different person may increase the likelihood that the unique aims and interests associated with that role will be given the attention that they require and will be vigorously pursued as the individuals filling different roles negotiate a common security plan based on their different (and sometimes potentially even competing) interests. If one person fills multiple roles, the negotiation and planning process can be short-circuited by this conflict of interest as the person decides to privilege one of his or her roles above the other(s).<sup>72</sup>

If one individual fills multiple roles during the operations and maintenance phase of the SDLC, this can also cause problems insofar as the effectiveness of some administrative, logical, and physical controls may be grounded in the fact that each individual within the organization is expected to fill only a single role, and disabling or bypassing the control would require collusion among two or more individuals; an individual who is simultaneously filling multiple roles may (if only temporarily) be able to singlehandedly bypass the control and compromise the information security of the entire system.

In the case of an advanced neuroprosthetic system, complications may arise from the fact that typically the role of serving as a device's human host is permanently filled by a single person – who may also be its sole operator and who has an intense interest in the safety and security of the device. In such circumstances, the host may fill multiple roles simultaneously, and he or she must be adequately trained and educated to understand the different aims and interests connected with different roles and the need to prudently balance the claims of competing interests when performing activities relating to the different roles.

### Roles and responsibilities for nonhuman agents?

While technological systems play key roles in the performance of many security activities, it is generally the human being who oversees the operation of that system who is said to possess responsibility for the activity and thus

---

<sup>72</sup> NIST SP 800-100 (2006), p. 68.

to fill a particular role. The extent to which legal and ethical responsibility for the performance of certain tasks could be attributed to a technological system such as an instantiation of artificially intelligent software, a social robot, or a sapient robotic network or swarm is a matter of ongoing debate.<sup>73</sup>

## Conclusion

As we have seen in this chapter, the work of ensuring information security for a neuroprosthetic system often involves collaboration among many individuals who fill different roles that give them responsibility for carrying out particular information security activities. In the following three chapters, we will explore in greater detail the nature and importance of many of these activities, which can be grouped into three main categories as management, operational, and technical controls.

---

<sup>73</sup> See, e.g., Coeckelbergh, “From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots” (2011); Calverley, “Imagining a non-biological machine as a legal person” (2008); Datteri, “Predicting the Long-Term Effects of Human-Robot Interaction: A Reflection on Responsibility in Medical Robotics” (2013); Hellström, “On the Moral Responsibility of Military Robots” (2013); Kuflik, “Computers in Control: Rational Transfer of Authority or Irresponsible Abdication of Autonomy?” (1999); Kirkpatrick, “Legal Issues with Robots” (2013); Stahl, “Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency” (2006); and Weber, “General Approaches for a Legal Framework” (2010).



## Chapter Seven

# Management Controls for Advanced Neuroprosthetics

Security controls can be understood as falling into three general classes of *management*, *operational*, and *technical* controls.<sup>1</sup> Throughout the next three chapters, we explore how such controls relate to advanced neuroprosthetic devices and systems by considering in detail the families of security controls that are listed and described in *NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, produced by the National Institute of Standards & Technology in 2013.

We address most of the security controls in the order in which they are listed in *NIST SP 800-53*, explaining how particular controls that were designed for use with general-purpose computing and information systems may either: 1) become *more critical* for ensuring information security when the information system to which the control is being applied is an advanced neuroprosthetic device; 2) become *less important* or potentially even inapplicable and irrelevant within the context of an advanced neuroprosthetic device; or 3) may take on a *new and radically* different form when applied to an advanced neuroprosthetic device. Some of the security controls listed in *NIST SP 800-53* are omitted and not explicitly addressed here, if their nature or importance does not significantly change when applied to advanced neuroprosthetic devices and systems. We begin our consideration of these issues in this chapter by focusing on management controls for advanced neuroprosthetics.

Management controls include activities such as **risk assessment, planning, system and services acquisition, and certification, accreditation, and security assessments**.<sup>2</sup> In the case of an advanced neuroprosthetic device, the device's manufacturer and designer would perform some of these tasks during the

---

<sup>1</sup> *NIST SP 800-100* (2006), p. 11.

<sup>2</sup> *NIST SP 800-100* (2006), p. 111.



process of determining the device's potential uses and targeted market segments, assessing the risks that the device and its users are likely to encounter, planning the device's security features, and ensuring the qualifications and expertise of personnel responsible for designing the device's security features. The users of neuroprosthetic devices (whether institutional users or individual consumers) may also carry out their own risk assessment and planning as part of their process of selecting and acquiring particular systems and services.

## **Risk assessment**

### **Security categorization<sup>3</sup>**

For an advanced neuroprosthetic system, security categorization includes classifying the system and its information not only in relation to requirements determined by laws, regulations, and organizational policies and ethical standards relating to computer equipment but also in accordance with those regulations and guidelines that apply to personal medical data, implantable medical devices, surgical procedures, psychological diagnostic and therapeutic procedures, and other relevant fields.<sup>4</sup>

### **Risk assessment<sup>5</sup>**

A risk assessment should be carried out (and updated as needed) for an information system and its operation as a whole as well as for relevant component devices and particular uses of the system, in order to analyze the "risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits."<sup>6</sup> Such assessments should identify both risks resulting from factors internal to the

---

<sup>3</sup> NIST SP 800-53, Rev. 4 (2013), p. F-151.

<sup>4</sup> For an overview of ethical issues with ICT implants – many of which are relevant for advanced neuroprosthetics – see Hildebrandt & Anrig, "Ethical Implications of ICT Implants" (2012). For ethical issues in information security more generally, see Brey, "Ethical Aspects of Information Security and Privacy" (2007). For regulatory issues, see Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); Mak, "Ethical Values for E-Society: Information, Security and Privacy" (2010); McGrath & Scanail, "Regulations and Standards: Considerations for Sensor Technologies" (2013); and Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010).

<sup>5</sup> NIST SP 800-53, Rev. 4 (2013), p. F-152.

<sup>6</sup> NIST SP 800-53, Rev. 4 (2013), p. F-152.

organization that will operate the device and internal to the device itself as well as risks resulting from external factors or agents.

In the case of advanced neuroprosthetic devices, the risk assessment should not be limited to evaluating the potential impact of the unauthorized use or alteration of information contained within the device itself but also the impacts of the possible unauthorized use or alteration of information (such as memories or sense data) which are not contained within the physical components of the device itself but which are received, generated, or transmitted by or stored within natural biological systems that belong to the device's human host and which are thus contained within the device-host system.<sup>7</sup>

### Vulnerability scanning<sup>8</sup>

In some circumstances, even the mere act of scanning an implanted neuroprosthetic device to identify vulnerabilities could be considered an invasive medical procedure and an infringement on the personal privacy of the human host in whom the device is implanted. In other circumstances, it could potentially be considered medical malpractice for an organization not to utilize all available means in probing neuroprosthetic devices implanted in its personnel to identify vulnerabilities, the breadth and depth of coverage, and the nature and extent of discoverable information within the devices and their connected systems that is potentially available to unauthorized parties.

### Technical surveillance countermeasures survey<sup>9</sup>

Technical surveillance countermeasures surveys are conducted in order “to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities.”<sup>10</sup> They are generally performed using a combination of intensive electronic testing, visual observation, and physical examination of information systems, the facilities in which they are housed, and the surrounding environment.<sup>11</sup>

In the case of advanced neuroprosthetics utilized by an organization, it may not always be legally, ethically, or practically feasible to conduct countermeasures surveys in all of the venues in which a neuroprosthetic device may operate (e.g., within the home of its human host), even with the advance

---

<sup>7</sup> See Chapter Three of this text for a discussion of information security for the device vs. the device-host system.

<sup>8</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-153.

<sup>9</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-155.

<sup>10</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-155.

<sup>11</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-155.

consent of the host. Surveillance countermeasures surveys must also be conducted in a way that does not create a danger of physical or psychological harm for the host of a neuroprosthetic device or for others. Finally, it should be noted that in some cases the efficacy of surveillance countermeasures surveys that are planned and conducted in conjunction with the human host of a neuroprosthetic device may be compromised by the fact that one form of implementing a “surveillance device” by adversaries would involve hacking a host’s existing sensory organs, memory systems, or other cognitive processes in order to gain access to data that was already being (or was at least capable of being) gathered by or stored in a host’s existing neuroprosthetic device.<sup>12</sup> In such a case, the adversary utilizing an existing neuroprosthetic device as a surveillance device may – through the device – gain advance notice of planned surveillance countermeasures surveys and be able to evade them through appropriate planning. Moreover, some kinds of technical surveillance countermeasures surveys may be able to detect the presence of a surveillance device that should not have been present at all but may have more difficulty detecting the fact that a human host’s neuroprosthetic device that was known to and whose presence was authorized by the organization had been hijacked or otherwise compromised by an adversary and was being (either temporarily, periodically, or permanently) employed by an unauthorized party as a surveillance device. It may be similarly difficult to detect situations in which an employee whose implanted neuroprosthetic device is known to (and perhaps even provided by) the organization is being utilized by the employee in an unauthorized way as a surveillance device, particularly if the patterns of device activity reflected in such unauthorized uses are generally consistent with those seen when the device is used for authorized purposes.

## Planning

### System security plan<sup>13</sup>

Development of an effective system security plan for certain kinds of neuroprosthetic devices may be complicated by the fact that the human host in whom a device is implanted either is not aware of the device’s existence or is not able – due to legal, ethical, or practical considerations – to participate constructively in execution of the system security plan. This may be the case, for example, in situations in which devices have been implanted in children,

---

<sup>12</sup> See Chapter Three of this text for a discussion of the possibility of adversaries accessing another individual’s neuroprosthetic device in order to create a surveillance instrument.

<sup>13</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-139-F-141.

persons who are in a coma, or individuals who are otherwise incapacitated, as well as in the case of some devices used for military or intelligence-gathering purposes in which the host's access to information about the device and its operations must be constrained. Significant questions relating to personal privacy, human autonomy, bioethics, and the ethics of technology arise in such situations that must be addressed.<sup>14</sup>

### Rules of behavior<sup>15</sup>

Under normal circumstances, the organization operating an information system may potentially unilaterally update the rules of behavior governing the use of that system and require all members of the organization to produce “a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior;”<sup>16</sup> an individual who declines to agree to the new rules of behavior may be denied access to the information system, removed from the organization, or potentially subjected to other disciplinary or personnel action as allowable by relevant law, regulations, employment agreements, and ethical guidelines. However, in the case of neuroprosthetic devices that have been implanted in the members of an organization and operated by that organization, it may be illegal, unethical, and impractical to attempt to force members to agree to new rules of behavior that are being unilaterally imposed by the organization after devices have already been implanted; it may also be impermissible to attempt to deactivate or remove such devices simply because the members decline to agree to the updated rules of behavior.

### Security concept of operations<sup>17</sup>

An organization's security concept of operations (or CONOPS) for an information system typically describes “how the organization intends to operate the system from the perspective of information security;”<sup>18</sup> any changes to the ongoing operations relating to the information system (and thus its CONOPS) will eventually be reflected in an updated system security plan, information security architecture, or other documents such as information security specifications governing specifications for future hardware and software acquisitions, SDLC materials, and systems engineering materials.<sup>19</sup> In the case

---

<sup>14</sup> See Bowman et al., “The Societal Reality of That Which Was Once Science Fiction” (2012), for a discussion of some such issues.

<sup>15</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-141.

<sup>16</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-141.

<sup>17</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-142.

<sup>18</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-142.

<sup>19</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-142.

of advanced neuroprosthetics, the CONOPS may also draw on (and changes to the CONOPS may need to be reflected in):

- **Biomedical and bioengineering specifications** that set operating parameters that should be maintained within the biological organism of a device's human host in order to ensure its safe and effective functioning.
- **Biocybernetic system architecture** documents that describe the processes of communication and control within and between the device and its human host.
- **Cognitive and noetic security plans** which describe and dictate the ways in which the privacy and autonomy of the mind of the device's human host (and the mind's integral cognitive processes) will be ensured.

### Information security architecture<sup>20</sup>

An information security architecture is designed to describe in a clear and coherent manner “the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information” and to explain “how the information security architecture is integrated into and supports the enterprise architecture.”<sup>21</sup> For an advanced neuroprosthetic device, the information security architecture not only supports and is integrated into the overall enterprise architecture of the organization operating the device but must also incorporate (or, in effect, function as) the biomedical security architecture, biomedical security architecture, and cognitive and noetic security architecture of the human being in whom the device is implanted.

### Central management<sup>22</sup>

In the case of neuroprosthetics operated by organizations with relevant technical and managerial capacity, it is feasible to maintain a single coherent, organization-wide system for designing, implementing, and managing security controls and processes.<sup>23</sup> In the case of neuroprosthetic devices that are sold to the general public as consumer electronics devices, the device-host

---

<sup>20</sup> NIST SP 800-53, Rev. 4 (2013), p. F-142.

<sup>21</sup> NIST SP 800-53, Rev. 4 (2013), p. F-142.

<sup>22</sup> NIST SP 800-53, Rev. 4 (2013), p. F-144.

<sup>23</sup> NIST SP 800-53, Rev. 4 (2013), p. F-144.

system constituted by an implanted device and its human host may not possess a single coherent, centrally-organized information security approach but may instead reflect a patchwork of diverse and unrelated (and potentially contradictory) information security mechanisms and procedures developed by the device's manufacturer, its OS developer, the application developers of programs installed on the device, and the device's human host.<sup>24</sup>

## System and services acquisition

### Allocation of resources<sup>25</sup>

When considering information security for neuroprosthetic devices, special care must be given in the case of devices that will be permanently implanted and may reside within and interact with the biological systems and cognitive processes of their human host for a period of years or decades, in order to ensure that the device's operator and (in a case in which the operator might declare bankruptcy, otherwise become incapable of providing information security services, or otherwise fail in its obligation to ensure the long-term safety and information security of the implanted device) the device's human host will be able to provide the resources needed in order to ensure the safe and secure long-term functioning of the device.

### System development life cycle<sup>26</sup>

The system development life cycle for neuroprosthetic devices should take into account the fact that once a device has been implanted into a human host, the organization operating the device may lose control over some or all aspects of the operations and maintenance phase and, in particular, the disposal phase for the device, insofar as it may not be legally, ethically, or practically feasible to carry out some kinds of activities (such as physically altering a device's integration with the neural circuitry of its human host or subjecting a device to removal or recall) without the consent of its host.

### Acquisition process<sup>27</sup>

An organization's acquisition process for advanced neuroprosthetics should not only define traditional functional, strength, and assurance requirements relating to information security for the device itself but also for the larger device-host system. Goals for the device-host system also include

---

<sup>24</sup> See the device ontology in Chapter Four of this text for a list of such relevant parties that can impact a neuroprosthetic device's information security and see Chapter Six for a discussion of the roles and responsibilities of such parties.

<sup>25</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-156.

<sup>26</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-157.

<sup>27</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-158-F-160.

preserving the cognitive and noetic security, privacy, and autonomy of the device's human host.

### **Information system documentation<sup>28</sup>**

An organization must acquire and, subsequently, appropriately secure documentation from neuroprosthetic devices' designers and manufacturers and OS developers regarding subjects such as high-level design principles, low-level design details, the functional properties of security controls built into the device and its OS, source code, external system interfaces, and the full features of and implications of using administrative accounts built into the device and its OS.<sup>29</sup> In the case of an advanced neuroprosthetic device, such documentation would also include recommendations and requirements regarding the biological systems and structures into which the device will be integrated, recommended methods for performing implantation and integration of the system into the host's neural circuitry, and circumstances in which implantation of a device into a particular host is contraindicated or deactivation or removal of the device is required.

### **Security engineering principles<sup>30</sup>**

In developing the designs and specifications for advanced neuroprosthetic devices, entirely new kinds of information system security engineering principles may need to be developed which incorporate considerations relating to cognitive and noetic security and the preservation of human agency and autonomy within a device-host system.

### **External information system services<sup>31</sup>**

When engaging external information system service providers in relation to advanced neuroprosthetics, an organization must be careful that the external service providers do not receive access to the biological processes or cognitive processes of devices' human hosts in a way that may be illegal or unethical; consent that has been given by the hosts for the organization to access and use information or to manipulate their internal biological or cognitive processes may or may not apply to external service providers acting on behalf of the organization. Moreover, it is not enough for an organization to satisfy itself that it does not possess conflicts of interest or other potentially

---

<sup>28</sup> NIST SP 800-53, Rev. 4 (2013), p. F-160-F-161.

<sup>29</sup> NIST SP 800-53, Rev. 4 (2013), p. F-161.

<sup>30</sup> NIST SP 800-53, Rev. 4 (2013), p. F-162.

<sup>31</sup> NIST SP 800-53, Rev. 4 (2013), p. F-162-F-164.

harmful characteristics that could impair or call into question its ability to ensure the information security of devices' human hosts; an organization should also seek and obtain assurance that potential external service providers do not possess conflicts of interest, ulterior motives, or other traits that may give reasons for neglecting or actively compromising the information security of neuroprosthetic devices' human hosts, either as a group or in specific cases (e.g., with regard to human hosts who are significant political, military, business, or entertainment figures).

### Developer configuration management<sup>32</sup>

Effective monitoring and supervision of developers' configuration management on the part of an organization is especially important in cases where the developer of, for example, the OS or software applications installed in implanted neuroprosthetic devices maintains direct access to the software and periodically pushes out software updates, patches, or configuration changes to devices that are implanted and in use.<sup>33</sup>

### Developer security testing and evaluation<sup>34</sup>

Some practices that an organization may typically require of third-party software providers – such as static code analysis<sup>35</sup> and manual code analysis<sup>36</sup> may not be relevant or possible in cases in which, for example, neuroprosthetic devices include physical neural networks that do not execute programs or code as traditionally understood.<sup>37</sup>

### PENETRATION TESTING<sup>38</sup>

The traditional conceptualization of penetration testing as either black-, gray-, or white-box testing takes on new aspects in the case of advanced neuroprosthetics. In a sense, it may be impossible for any developer (or outside assessor acting on behalf of the developer) playing the role of an adversary to conduct full white-box testing, insofar as that would entail being given all available schematics, documentation, and information relating to the functioning of the system – and in the case of an advanced neuroprosthetic device

<sup>32</sup> NIST SP 800-53, Rev. 4 (2013), p. F-164-F-166.

<sup>33</sup> See Chapter Six of this text for a discussion of the roles and responsibilities of OS and application developers for neuroprosthetic devices.

<sup>34</sup> NIST SP 800-53, Rev. 4 (2013), p. F-166-F-169.

<sup>35</sup> NIST SP 800-53, Rev. 4 (2013), p. F-166.

<sup>36</sup> NIST SP 800-53, Rev. 4 (2013), p. F-167.

<sup>37</sup> For a discussion of, e.g., neuroprosthetic devices based on physical neural networks that do not execute traditional programs, see the device ontology in Chapter Four of this text.

<sup>38</sup> NIST SP 800-53, Rev. 4 (2013), p. F-168.



some such information and resources may be stored in the mind of the device's host in a way that cannot be conveyed to any other party; in that case, only a device's human host could (if sufficiently skilled) perform true white-box penetration testing.

#### **ATTACK SURFACE REVIEWS<sup>39</sup>**

An organization may conduct attack surface reviews to identify “exposed areas that make those systems more vulnerable to cyber attacks;” such attack surfaces include “any accessible areas where weaknesses or deficiencies in information systems (including the hardware, software, and firmware components) provide opportunities for adversaries to exploit vulnerabilities.”<sup>40</sup> In the case of advanced neuroprosthetics, attack surfaces may comprise not only the hardware and software components of the device itself but also anatomical structures, biological systems, and psychological and cognitive processes within a device's human host.

### **Supply chain protection**

#### **LIMITATION OF HARM<sup>41</sup>**

It is possible that adversaries may choose to identify and target an organization's supply chain of components or services needed for the design, production, implementation, maintenance, or operation of organizational information systems rather than directly targeting the information systems themselves. *NIST SP 800-53* notes that “Supply chain risk is part of the advanced persistent threat (APT)”<sup>42</sup> that organizations face. An adversary could potentially execute such an attack by compromising a supplier and covertly corrupting or manipulating the supplier's production process, so that components produced by the supplier for the organization have been produced using improper materials that will disintegrate, break, or otherwise fail (or, in the case of an advanced neuroprosthetic system, potentially poison the device's host or release other biologically or psychologically active agents into the host's body) after the information system is in use, or components may have been corrupted with computer viruses or worms or designed with unauthorized backdoors that will allow adversaries unauthorized access to the

---

<sup>39</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-168.

<sup>40</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-168. See Chapter Two of this text for a discussion of vulnerabilities of neuroprosthetic devices. For vulnerabilities in IMDs generally, see Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010).

<sup>41</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-170.

<sup>42</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-170.

system after it is in use.<sup>43</sup> In the case of some advanced neuroprosthetic devices, the number of suppliers producing certain necessary components may (at least initially) be quite small: such a phenomenon is disadvantageous, insofar as it bars an organization from pursuing the typical approach of minimizing supply chain risk by acquiring components from multiple suppliers, although it is potentially advantageous, insofar as it allows an organization to concentrate its information security resources and efforts on securing the operations of just a single supplier or small group of suppliers.

#### **USE OF ALL-SOURCE INTELLIGENCE<sup>44</sup>**

The potential widespread use of advanced neuroprosthetics by the public (including by employees and customers of suppliers) may provide organizations with a new element to incorporate into all-source intelligence analysis: namely, the thoughts, memories, perceptions, plans, and emotions of individuals associated with current or potential suppliers that are publically shared by these persons through neuroprosthetically enabled social networks. This would represent a potentially deeper and more sophisticated source of information and analysis than can be obtained, for example, from the contemporary analysis of social media posts.

#### **OPERATIONS SECURITY<sup>45</sup>**

An organization may utilize operations security (or OPSEC) practices and safeguards in relation to current and potential suppliers.<sup>46</sup> In this context,

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to: (i) identify those actions that can be observed by potential adversaries; (ii) determine indicators that adversaries might obtain that could be interpreted or pieced together to derive critical information in sufficient time to cause harm to organizations; (iii) implement safeguards or countermeasures to eliminate or reduce to an acceptable level, exploitable vulnerabilities; and (iv) consider how aggregated information may compromise the confidentiality of users or uses of the supply chain.<sup>47</sup>

---

<sup>43</sup> Regarding backdoors intentionally built into implantable medical devices to allow emergency access to medical personnel – which could potentially be exploited by sufficiently knowledgeable adversaries – see Clark & Fu, “Recent Results in Computer Security for Medical Devices” (2012); Halperin et al., “Security and privacy for implantable medical devices” (2008); and Chapter Three of this text.

<sup>44</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-171.

<sup>45</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-171.

<sup>46</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-171.

<sup>47</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-171.

As employed by some organizations, OPSEC practices and tactics may sometimes lead an organization to “withhold critical mission/business information from suppliers and may include the use of intermediaries to hide the end use, or users, of information systems, system components, or information system services.”<sup>48</sup>

Before they can be implemented, careful attention must be given to the legal and ethical implications of such OPSEC practices in the case of advanced neuroprosthetic devices. For example, a supplier that is led to believe that it is producing components for use in neuroprosthetic devices to be implanted in mice for experimental research may utilize a different level of care in producing the components (and, indeed, may make a different decision about whether to enter into a contract to supply the components) than they would have done if they had been aware of the fact that their components would be incorporated into neuroprosthetic devices to be implanted in human hosts for use in their performance of critical tasks – even if the suppliers’ knowledge of the true circumstances of the devices’ ultimate use would not in any way have affected the specifications of the components that the organization had asked the supplier to produce. Complex problems involving legal liability, moral responsibility, corporate social responsibility, and informed decision-making can arise if OPSEC activities prevent the free and robust flow of accurate information between an organization, its suppliers, and other parties involved with the development and implementation of advanced neuroprosthetic devices.

On the other hand, in situations in which the personal medical data and sensitive information about the cognitive processes (including thoughts, memories, and emotions) of particular human hosts is involved, an organization may have a legal and ethical responsibility not only to conceal the detailed information that is received, stored, generated, or transmitted by the neuroprosthetic devices that it operates but even any incidental or circumstantial information that could potentially be used by suppliers to ascertain (or even guess at) the identity of a device’s human host.<sup>49</sup> This may be especially important in cases in which a host is a significant political, business, artistic, or entertainment figure, a military or police operative, or some other

---

<sup>48</sup> NIST SP 800-53, Rev. 4 (2013), p. F-171.

<sup>49</sup> For discussions of such issues, see Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants” (2012); McGee, “Bioelectronics and Implanted Devices” (2008); Shoniregun et al., “Introduction to E-Healthcare Information Security” (2010); Hildebrandt & Anrig, “Ethical Implications of ICT Implants” (2012); and Brey, “Ethical Aspects of Information Security and Privacy” (2007).

individual whom unauthorized parties may have a particular interest in observing, stealing information from, blackmailing, extorting, or otherwise compromising or exploiting.

#### IDENTITY AND TRACEABILITY<sup>50</sup>

For neuroprosthetic devices that are housed permanently within the body of a human host and that cannot easily be physically inspected or extracted, the confirmation of identity and traceability of such devices and their components may need to be accomplished using technologies such as RFID tags<sup>51</sup> that can be checked wirelessly by a reader external to the host's body. In the case of some kinds of advanced neuroprosthetics utilizing biological components, it may be possible to incorporate identifying marks, codes, supporting documentation, and other information into the genetic sequences of the biological material.<sup>52</sup>

#### Trustworthiness<sup>53</sup>

The trustworthiness of an information system depends both on 1) the set of features, mechanisms, and procedures built into the device and its operating environment that constitute the system's *security functionality*, and 2) the *security assurance* which allows the organization to believe that the potential benefits offered by the security functionality are actually being obtained through a proper and effective implementation of the functionality.<sup>54</sup>

It should be noted that in at least some respects, some kinds of advanced neuroprosthetic devices may be inherently *untrustworthy*. For example, certain kinds of devices that include a physical neural network and which interact closely with the natural memory systems of the human mind to expand or support the mind's long-term memory storage may be subject to the same kind of mnemonic compression, distortion, and gradual information degradation that is observed with natural human memories.<sup>55</sup>

#### Criticality analysis<sup>56</sup>

In the case of advanced neuroprosthetic devices, some device components might be designated as critical not because they directly secure information

---

<sup>50</sup> NIST SP 800-53, Rev. 4 (2013), p. F-172.

<sup>51</sup> NIST SP 800-53, Rev. 4 (2013), p. F-172.

<sup>52</sup> For such possibilities, see Church et al., "Next-generation digital information storage in DNA" (2012).

<sup>53</sup> NIST SP 800-53, Rev. 4 (2013), p. F-173.

<sup>54</sup> NIST SP 800-53, Rev. 4 (2013), p. F-173.

<sup>55</sup> See Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

<sup>56</sup> NIST SP 800-53, Rev. 4 (2013), p. F-174.

contained within a device but because they supports the physical and psychological health and safety of the device's human host, thereby indirectly ensuring the security of information held within the natural cognitive processes of the host's mind.<sup>57</sup>

### Development process, standards, and tools<sup>58</sup>

With advanced neuroprosthetic devices, it is especially important that suppliers and developers follow a well-defined and thoroughly documented development process for components and services, since in the case of unforeseen operational emergencies (e.g., a critical negative impact on the health or biological processes of a device's human host that arises unexpectedly) it may be necessary to quickly retrace and analyze steps in the development of the component or service in order to formulate a response that can prevent serious harm to the device's host or to others.

### THREAT MODELING / VULNERABILITY ANALYSIS<sup>59</sup>

In some cases, the ability of developers to perform effective threat modeling and vulnerability analysis for advanced neuroprosthetic devices (or their constituent components or software) that are under development may be impeded by the fact that a device's functional and operational characteristics do not become clear until it is implanted in a particular human host and integrated with the host's neural circuitry, insofar as a device may be largely passive in nature, and its functional characteristics are determined largely by the unique traits (e.g., memories, thoughts, or volitions) of the mind of its human host.<sup>60</sup>

### USE OF LIVE DATA<sup>61</sup>

The use of live data during the development and testing of information systems is generally discouraged, as storing information within systems whose security functionality is not yet assured and utilizing the information in a way unprotected by an organization's existing information security mechanisms and procedures creates a significant risk.<sup>62</sup> However, with some

---

<sup>57</sup> See Chapter Three of this text for the need to secure both a device and its larger device-host system.

<sup>58</sup> NIST SP 800-53, Rev. 4 (2013), p. F-174.

<sup>59</sup> NIST SP 800-53, Rev. 4 (2013), p. F-175.

<sup>60</sup> See Chapter One of this text for a discussion of passive neuroprosthetics and Chapter Three for a discussion of the classification of vulnerabilities and threats relating to advanced neuroprosthetic devices.

<sup>61</sup> NIST SP 800-53, Rev. 4 (2013), p. F-176.

<sup>62</sup> NIST SP 800-53, Rev. 4 (2013), p. F-176.

kinds of neuroprosthetic devices it may be impossible to avoid the use of live data even during the initial development and testing phases – e.g., in cases in which a neuroprosthetic device is not fully assembled in an external facility and then implanted whole into the body of a human host but is instead assembled (or, if it utilizes biological components, even “grown”<sup>63</sup>) within the body of its human host, piece by piece – perhaps through the use of nanorobots<sup>64</sup> or other technologies). In such cases, the development process for each particular neuroprosthetic device is unique and depends on (and is guided by) the immediate feedback provided by live data generated by the biological or cognitive processes the device’s human host.

## Developer security architecture and design

### FORMAL POLICY MODEL<sup>65</sup>

The kinds of formal policy modeling tools traditionally used to model practices such as nondiscretionary access control policies with formal languages<sup>66</sup> may have limited applicability for some kinds of advanced neuroprosthetic devices. For example, for some kinds of neuroprosthetic devices that comprise physical neural networks or swarms of nanorobot elements may not include nondiscretionary access controls that can easily be modeled; in the case of devices that are passively controlled by the minds and cognitive processes of their human hosts, a system’s security controls may be entirely discretionary and controlled by the decision-making and volition of the device’s human host.

It may be possible to develop new kinds of formal policy models and modeling languages that address the unique information security situations of advanced neuroprosthetic devices (including the typically important goal of preserving autonomy and agency for the device-host system as a whole).

### CONCEPTUALLY SIMPLE DESIGN<sup>67</sup>

Requirements that developers develop systems that utilize “a complete, conceptually simple protection mechanism with precisely defined semantics”

---

<sup>63</sup> For the possibility of neuroprosthetic devices involving biological components, see Merkel et al., “Central Neural Prostheses” (2007). For a hybrid biological-electronic interface device (or “cultured probe”) that includes a network of cultured neurons on a planar substrate, see Rutten et al., “Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe” (2007). Hybrid biological-electronic interface devices are also discussed by Stieglitz in “Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems” (2007).

<sup>64</sup> See Pearce, “The Biointelligence Explosion” (2012).

<sup>65</sup> NIST SP 800-53, Rev. 4 (2013), p. F-178.

<sup>66</sup> NIST SP 800-53, Rev. 4 (2013), p. F-178.

<sup>67</sup> NIST SP 800-53, Rev. 4 (2013), p. F-179.

may be difficult to realize in situations in which protection mechanisms may, for example, be implemented and directed largely in a discretionary manner by the mind of the human host in whom a device is implanted.

#### **STRUCTURE FOR LEAST PRIVILEGE<sup>68</sup>**

“Least privilege” may have a unique meaning in the case of some advanced neuroprosthetics whose human hosts are legally and ethically expected to possess full privileges for all aspects of a device’s operation and who may determine – not during the development stage of the device but only after its implementation – how to assign privileges to other parties, subject to regular unilateral modification according to the hosts’ wishes.

### **Tamper resistance and detection**

#### **MULTIPLE PHASES OF SDLC<sup>69</sup>**

The tamper-resistance mechanisms that are legally and ethically permissible and practically feasible during the pre-implantation production and testing of a neuroprosthetic device may be entirely different from those that are possible and desirable during the operations and maintenance or disposal phases of the device’s SDLC.

#### **INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES<sup>70</sup>**

The inspection of a neuroprosthetic device after its implantation may require the express consent of the device’s host. There is a danger that if the information security of an already-implanted device has indeed been compromised by an adversary – and the device is able to influence or exercise control over relevant biological or cognitive processes – then the human host may decline to express consent to an inspection not because the host has decided to reject the inspection through an act of his or her autonomy agency and volition but because the adversary has utilized control over the compromised device in a way that blocks the host from expressing agreement to an inspection.<sup>71</sup>

### **Component authenticity<sup>72</sup>**

---

<sup>68</sup> NIST SP 800-53, Rev. 4 (2013), p. F-179.

<sup>69</sup> NIST SP 800-53, Rev. 4 (2013), p. F-180.

<sup>70</sup> NIST SP 800-53, Rev. 4 (2013), p. F-180.

<sup>71</sup> See Chapter Three of this text for the related possibility of a neuroprosthetic device that unintentionally traps the mind of its human host within a “zombie-like” device-host system in which the host is unable to express his or her thoughts or volitions using motor activity.

<sup>72</sup> NIST SP 800-53, Rev. 4 (2013), p. F-180.

Preventing the use of counterfeit components is especially important in the case of neuroprosthetic devices in which the discovery that counterfeit components (which may potentially be constructed from toxic materials or of otherwise substandard quality) had been used in a neuroprosthetic device may necessitate complex, expensive, dangerous, and legally and ethically fraught surgery to extract the device and replace the components.<sup>73</sup>

### Customized development of critical components<sup>74</sup>

For kinds of some neuroprosthetic devices, the in-house development of customized, nonstandard components (which may be less vulnerable to standard attacks that adversaries may be likely to employ) may be a natural and even necessary aspect of a device's development. For example, in the case of neuroprosthetic devices that utilize biological components that incorporate the host's DNA or whose security functionality depends on unique features of the host's mind (such as memories unique to that host<sup>75</sup>), each device may in effect be deeply customized and nonstandard.

### Unsupported system components<sup>76</sup>

Typical best practices of removing and replacing system components once they are no longer supported by their designer, manufacturer, or provider may be difficult or impossible to implement in the case of devices that have been implanted in a human host and whose removal would require complex, expensive, or dangerous surgical procedures or would otherwise create a possibility of physical or psychological harm for a device's host.

## Certification, accreditation, and security assessments

### System interconnections<sup>77</sup>

If multiple kinds of neuroprosthetics are available for acquisition, installation, and use by members of the general public as consumer electronics, it may be difficult or impossible to predict the ways in which multiple devices may be combined and interconnected within a single human host. Even if devices do not directly interconnect with one another, they may indirectly

---

<sup>73</sup> For medical risks relating to surgery for the implantation of even "simple" implants such as passive RFID devices, see Rotter et al., "Passive Human ICT Implants: Risks and Possible Solutions" (2012).

<sup>74</sup> NIST SP 800-53, Rev. 4 (2013), p. F-181.

<sup>75</sup> See Chapter Three of this text for a discussion of the possibility of using a host's thoughts and memories as biometric access controls.

<sup>76</sup> NIST SP 800-53, Rev. 4 (2013), p. F-182.

<sup>77</sup> NIST SP 800-53, Rev. 4 (2013), p. F-57-F-58.



interconnect through the host's brain and mind, which can serve as a bridge allowing information to flow between devices and influence one another.

## Penetration testing

### **INDEPENDENT PENETRATION AGENT OR TEAM<sup>78</sup>**

Allowing penetration testing by independent agents or groups may create special dangers, insofar as independent agents who lack full access to information about the nature of a neuroprosthetic device and its human host may inadvertently employ penetration technologies or techniques that are especially likely to cause harm to that host. On the other hand, independent agents are free from conflicts of interest that may arise with penetration testing conducted by an organization's internal personnel.

### **RED TEAM EXERCISES<sup>79</sup>**

The potential use of penetration testing to identify vulnerabilities or test the resistance of an advanced neuroprosthetic system that is in use within a human host to hostile cyberattacks, social engineering, espionage, and other efforts at compromising information security must be carefully considered, given the possibility that such testing (whether or not it is successful in exploiting vulnerabilities) may cause physical or psychological harm to the device's host or others. Legal and ethical questions arise surrounding the extent to which penetration testing may be conducted on a neuroprosthetic device that has already been implanted in a human host; however, in some cases it may be impossible to accurately simulate the performance of an implantable device outside of the unique circumstances of its implantation within its particular human host. Moreover, if vulnerabilities indeed exist, penetration testing may allow them to be discovered by the neuroprosthetic device's operator and addressed before they can be exploited by hostile outside parties who might intentionally exploit them to inflict maximum possible damage to the device's human host.

---

<sup>78</sup> NIST SP 800-53, Rev. 4 (2013), p. F-62.

<sup>79</sup> NIST SP 800-53, Rev. 4 (2013), p. F-62.

## Chapter Eight

# Operational Controls for Advanced Neuroprosthetics

In this chapter we continue our exploration of how security controls relate to advanced neuroprosthetic devices and systems by considering in detail the families of security controls listed in *NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, produced by the National Institute of Standards & Technology in 2013. As in the previous chapter, we explain how particular controls that were designed for use with general-purpose computing and information systems may either: 1) become *more critical* for ensuring information security when the information system to which the control is being applied is an advanced neuroprosthetic device; 2) become *less important* or potentially even inapplicable and irrelevant within the context of an advanced neuroprosthetic device; or 3) may take on a *new and radically* different form when applied to an advanced neuroprosthetic device. In this chapter we focus on operational controls for advanced neuroprosthetics.

Operational controls include **personnel security, physical and environmental protection, contingency planning, configuration management, maintenance, system and information integrity, media protection, incident response, and awareness and training.**<sup>1</sup>

In the case of an advanced neuroprosthetic device, such activities do not become relevant only after the item is in use; such activities must be utilized by the device's manufacturer throughout the process of design, production, and distribution in order to ensure that the device ultimately implanted in a consumer indeed reflects the security principles and features intended by the manufacturer and that the device's security has not been compromised, e.g., through the surreptitious addition of malware or the theft of design specifications or proprietary diagnostic or management tools that could be used by

---

<sup>1</sup> *NIST SP 800-100* (2006), p. iii.

competing companies or criminal enterprises to undermine the device's security.

Operational controls such as maintenance become essential after a device is being utilized within its human host. Although the device may appear to be functioning well even in the absence of ongoing maintenance, it is still crucial that end users follow ongoing maintenance protocols developed by the device's manufacturer or the IT and InfoSec personnel of the user's institution, as the failure to apply, e.g., regular security patches and software upgrades provided by the manufacturer may lead to the device operating with known vulnerabilities that can be exploited by unauthorized parties to compromise the user's security. Proper training of the host and user is also essential, in order to ensure that the device is used in a way that optimizes both its safety, security, and utility and which avoids the creation of unintended security vulnerabilities.<sup>2</sup>

## Personnel security

### Position risk designation<sup>3</sup>

For advanced neuroprosthetic systems, the risk designation for positions must take into account not only the extent to which a position's occupant will be able to directly access information stored within a device and within the natural biological systems of the device's human host but also the extent to which the position's occupant can indirectly alter, damage, or destroy information stored within a device or its host's biological systems by operating the device or interacting with or controlling the host in such a way alters or affects natural or artificial systems within the host's body that are not directly connected to the neuroprosthetic device but which can have an impact on the confidentiality, availability, or integrity of information stored within the device or its human host. For example, the position of a technician who can alter a device's settings in such a way that causes the device's host to enter a comatose state may require a high risk designation, even if the position's occupant does not have any direct ability to retrieve or interpret information stored within the device or the host's natural memory systems.

---

<sup>2</sup> For factors that might cause the host of an implanted device to intentionally ignore, disable, or otherwise subvert a device's security features and mechanisms – even when he or she realizes that this might put him or her at greater risk of harm – see Denning et al., “Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010).

<sup>3</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-145.

## Personnel screening

### **CLASSIFIED INFORMATION<sup>4</sup>**

In the case of advanced neuroprosthetic systems, it may sometimes occur that neuroprosthetic devices are being used by their operating organization to gather classified or sensitive information which the device's human hosts are not themselves authorized to access or possess; the legal and ethical conditions governing such activities should be carefully clarified.

### **FORMAL INDOCTRINATION<sup>5</sup>**

Formal training for the hosts of neuroprosthetic devices regarding the legal and ethical frameworks governing the functioning of their devices and their relationships to classified or sensitive information may be necessary, for example, if a host possesses an artificial eye or other neuroprosthetic that is continuously recording, uploading, and potentially making publicly available information received from external environmental phenomena surrounding the host or from the host's internal cognitive processes.

## Personnel termination<sup>6</sup>

Standard procedures upon termination of the employment of an organization's member may include action by the organization that "Disables information system access" previously enjoyed by the employee within a specified time period, "Terminates/revokes any authenticators/credentials associated with the individual," "Retrieves all security-related organizational information system-related property," and "Retains access to organizational information and information systems formerly controlled by terminated individual."<sup>7</sup> The ability of an organization to carry out such actions in the case of an organizational information system that takes the form of a neuroprosthetic device implanted in the (former) employee may be significantly constrained by legal, ethical, and practical considerations.

For example, even if an employee had signed an employment contract or agreement clearly specifying that any devices subsequently implanted in the employee by the organization (and all information contained within them) were property of the organization and that the organization enjoyed the right to reclaim such devices at information any time, the ability of the organization to enforce the agreement and reclaim an implanted device through forcible surgical extraction would be legally and ethically doubtful, at best, although the employee could potentially be subject to civil action for theft or

---

<sup>4</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-146.

<sup>5</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-146.

<sup>6</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-147.

<sup>7</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-147.

conversion. Moreover, even if it is technologically possible for the organization to execute such an action by sending remote instructions to a device, an organization may not have a legal or ethical ability to forcibly reclaim a neuroprosthetic device or to destroy all of the information contained on it (such as thoughts or memories of the device's host), even if an employment agreement was unilaterally breached or terminated by the device's host in contravention of the agreement's terms and conditions.

#### **POST-EMPLOYMENT REQUIREMENTS<sup>8</sup>**

Automated systems may be employed to ensure that former employees are, for example, not able to make use of classified or sensitive information contained within neuroprosthetic devices that had been employed within them by their former employer, or even to utilize the devices at all. If a neuroprosthetic device has been designed and constructed in such a way that ongoing proactive authorization or support from the organization employing the device's host (e.g., wireless signals sent to the device from an external organizational information system) are required in order for the device to function or for its contained information to be accessible, the withdrawal of such authorization or support upon termination of an employee may constitute a practice that is legally and ethically permissible: in its natural state (i.e., in the absence of such signals or support) the device is nonfunctional, and the organization has no obligation to provide such ongoing support.<sup>9</sup> On the other hand, the situation becomes more legally and ethically complex if an implanted neuroprosthetic device's natural state is one in which the device functions nominally and information contained within it is available to the device's host, and the functioning of the device (and availability of its contained information) can only be suppressed by the organization through the ongoing application of some proactive measure – such as bombarding the host's body with electromagnetic impulses that jam the device's communications or otherwise disrupt its operation. The legal, ethical, and practical ability of an organization to carry out such measures may be severely constrained.

---

<sup>8</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-147.

<sup>9</sup> See the discussion in Chapter Three of this text of proposed schemes that utilize external hardware tokens, cloaking devices, or gateway devices whose presence causes an implanted medical device to behave in a particular way during emergency (or non-emergency) situations. Employers could potentially develop similar systems in which the employer could disable an implanted neuroprosthetic device or cause it to “fail closed” not by physically accessing the device itself or even wirelessly sending the device a command to disable itself (which may not be legally or ethically possible) but simply by confiscating, disabling, or failing to renew some external token or device in the possession of the implanted neuroprosthetic device's host that is needed in order to prolong the functioning of the implanted device.

### Access agreements<sup>10</sup>

Organizational access agreements may include components such as “non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.”<sup>11</sup> In the case of advanced neuroprosthetic devices, such agreements may be designed to protect the interests of multiple parties; for example, device designers and manufacturers, OS and software developers, and device operators may wish to ensure that devices’ human hosts will not misuse information that they acquire through their possession of and interaction with the device, and the devices’ human hosts may wish to ensure the confidentiality, possession, and legal ownership of sensitive information (e.g., relating to their biological or cognitive processes) that the devices may acquire or information (such as ideas, memories, inventions, discoveries, or artistic creations) that may be generated by the host’s mind with the assistance of the device.

### Personnel sanctions<sup>12</sup>

On the one hand, in order to ensure the security of highly sensitive information regarding the biological processes or cognitive activity of human hosts in whom neuroprosthetic devices are implanted, it may be necessary to enact a stringent formal sanctions process to discipline individuals within an organization who disregard or violate established information security procedures. On the other hand, there may be significant legal and ethical issues that complicate an organization’s ability to discipline the human host of a neuroprosthetic device who violates organizational information security procedures, especially if those procedural requirements have been unilaterally imposed by an organization subsequent to a device’s implantation or otherwise enacted without the full informed consent of the device’s host.

## Physical and environmental protection

### Physical access authorizations<sup>13</sup>

In the case of neuroprosthetics operated by large institutions (e.g., those operated by a military or intelligence agency for intelligence-gathering purposes), the organization may maintain comprehensive and detailed records of which human beings are serving as the hosts for which devices; no other human beings are authorized to serve as the hosts for those devices, and the

---

<sup>10</sup> NIST SP 800-53, Rev. 4 (2013), p. F-148.

<sup>11</sup> NIST SP 800-53, Rev. 4 (2013), p. F-148.

<sup>12</sup> NIST SP 800-53, Rev. 4 (2013), p. F-150.

<sup>13</sup> NIST SP 800-53, Rev. 4 (2013), p. F-127-F-128.

list of other individuals (e.g., organizational medical personnel) who are authorized to gain physical access to the devices is limited. On the other hand, with neuroprosthetic devices that are sold to the public through retail outlets as consumer electronics devices, there may be no reliable centralized record of which devices are implanted in which human beings and who is a device's "authorized" operator.

### Physical access control<sup>14</sup>

Maintaining physical access control is a challenge for advanced neuroprosthetic devices. The fact that a device is implanted within the body of a human host creates a practical, legal, and ethical obstacle that may prevent casual attempts by unauthorized parties to access the device: a neuroprosthetic unit that is implanted deep within a host's brain and possesses no external physical access ports is more difficult to physically access than a computer sitting on a desktop in an exposed workplace environment.<sup>15</sup> On the other hand, the fact that a neuroprosthetic device is implanted in a human host who can conceivably take it anywhere in the world – and who could potentially be abducted and forcibly restrained or transported – increases the opportunities to gain physical access to the device for unauthorized parties that have sufficient means and motivation, especially if a device possesses visible and easily accessible external slots, ports, or other physical access points.

### CONTINUOUS GUARDS/ALARMS/MONITORING<sup>16</sup>

In the case of implantable neuroprosthetic devices, it may be possible to use one device as a "guard" that monitors physical access to other devices implanted within the same human host.<sup>17</sup>

### LOCKABLE CASINGS<sup>18</sup>

Depending on the nature of a neuroprosthetic device, it may be necessary to ensure that legitimate, licensed emergency personnel have a way to unlock

---

<sup>14</sup> NIST SP 800-53, Rev. 4 (2013), p. F-128-F-129.

<sup>15</sup> See the device ontology in Chapter Four in this text for ways in which the information security of a neuroprosthetic device can be affected by the device's physical structure and its location within or in relation to its host's body.

<sup>16</sup> NIST SP 800-53, Rev. 4 (2013), p. F-129.

<sup>17</sup> See the related discussion in Chapter Three of this text of proposed schemes for emergency access to IMDs that utilize external cloaking devices or gateway devices to mediate, limit, or control access to an implanted device.

<sup>18</sup> NIST SP 800-53, Rev. 4 (2013), p. F-129.

or bypass lockable casings in order to physically access a device when providing emergency medical treatment to its human host.<sup>19</sup>

#### **TAMPER PROTECTION<sup>20</sup>**

Tamper-detection seals and anti-tamper coatings<sup>21</sup> may be utilized to prevent unauthorized access to a neuroprosthetic device's internal components or to ensure that if such components *have* been accessed by an unauthorized party, evidence of that unauthorized access will be visible to the next authorized party who conducts routine maintenance operations on or provides other service for the device.<sup>22</sup>

#### **FACILITY PENETRATION TESTING<sup>23</sup>**

In the case of advanced neuroprosthetic devices, it may or may not be possible for a device's operator to conduct penetration testing that involves "unannounced attempts to bypass or circumvent security controls associated with physical access points,"<sup>24</sup> if such operations create a risk that physical or psychological harm may result to a device's human host or to others.

### **Access control for output devices<sup>25</sup>**

Some neuroprosthetic devices not only include (or are connected to) traditional output devices such as radio transmitters or monitors; they are also linked to "output devices" such as the voicebox, facial muscles, hands, and other motor organs of their human host, which can be used to produce output in the form of speech, facial expressions, hand gestures, or typed or written communication.<sup>26</sup> Attempting to limit the host's use of such output systems may not be legally or ethically appropriate.

### **Monitoring physical access**

---

<sup>19</sup> For a discussion of emergency access to implantable neuroprosthetic devices, see Chapter Three of this text as well as Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012); Rotter & Gasson, "Implantable Medical Devices: Privacy and Security Concerns" (2012); and Halperin et al., "Security and privacy for implantable medical devices" (2008).

<sup>20</sup> NIST SP 800-53, Rev. 4 (2013), p. F-129.

<sup>21</sup> NIST SP 800-53, Rev. 4 (2013), p. F-129.

<sup>22</sup> The systems described in Chapter Three of this text for providing audible – rather than visible – alerts to a device's host when attempts are made to wirelessly access the device constitute another kind of anti-tampering mechanism.

<sup>23</sup> NIST SP 800-53, Rev. 4 (2013), p. F-130.

<sup>24</sup> NIST SP 800-53, Rev. 4 (2013), p. F-130.

<sup>25</sup> NIST SP 800-53, Rev. 4 (2013), p. F-130-F-131.

<sup>26</sup> See the device ontology in Chapter Four of this text for a discussion of different output mechanisms for neuroprosthetic devices.



**INTRUSION ALARMS / SURVEILLANCE EQUIPMENT<sup>27</sup>**

Multiple neuroprosthetic devices may be able to create a body area network (BAN) or body sensory network (BSN) in which devices conduct mutual surveillance, monitor one another's status, and identify physical intrusions into their host's body or bodily systems.

**AUTOMATED INTRUSION RECOGNITION/RESPONSES<sup>28</sup>**

The use of automated mechanisms to detect intrusions into a device or the surrounding body of its human host and to initiate particular response actions must be undertaken carefully, insofar as some forms of intrusion (e.g., medical procedures) may be done with the host's consent and at his or her direct request, and automated responses could potentially cause physical or psychological harm if initiated while the host was in the midst of performing or undergoing some critical activity or otherwise at a time not desired by the host.

**VIDEO SURVEILLANCE<sup>29</sup>**

In the case of some neuroprosthetic devices such as artificial eyes, the device itself may be able to provide video surveillance to the device's operator that records whether anyone has gained physical access to the device – with the caveat that if the device's security had already been compromised through some other means (e.g., if it had been hacked through use of software that had been installed on the device through a wireless connection), it may not be possible to trust the accuracy or integrity of any video stream being provided by the device, as that imagery could be fabricated or altered.<sup>30</sup>

An artificial eye may also be able to provide video surveillance that will allow operators to determine whether any parties have acquired physical access to other neuroprosthetic devices implanted in the same host or, potentially, in other persons who are within the artificial eye's field of vision.

**Visitor access records<sup>31</sup>**

---

<sup>27</sup> NIST SP 800-53, Rev. 4 (2013), p. F-131.

<sup>28</sup> NIST SP 800-53, Rev. 4 (2013), p. F-131.

<sup>29</sup> NIST SP 800-53, Rev. 4 (2013), p. F-132.

<sup>30</sup> For the possibility that a neuroprosthetic device that was designed to receive raw data from the external environment could have that data replaced with other data transmitted from some external information system, see Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012). Regarding the possibility that neuroprosthetic devices could be used to provide false data or information to their hosts or users, see also McGee, "Bioelectronics and Implanted Devices" (2008), p. 221.

<sup>31</sup> NIST SP 800-53, Rev. 4 (2013), p. F-132.

It may be appropriate for the organization operating a neuroprosthetic device to record the identities and other details of individuals who gain direct physical access to the device itself, however it may be legally or ethical questionable for the organization to record and archive details regarding the circumstances and identities of all individuals who gain physical access to the device's host more generally (e.g., through face-to-face meetings or in other ways).

### Power equipment and cabling<sup>32</sup>

Providing an adequate and reliable power supply that is protected against intentional or unintentional damage or destruction is a major challenge for the designers and operators of advanced neuroprosthetics. Some devices may be able to draw on natural power sources that are present in (or can be provided through) the natural biological systems of their human host. Such “energy harvesting” systems for implantable devices already exist. Some gather energy from sources such as the body heat or kinetic energy from movement of their host's body, and can often produce more than 10 milliwatts of power.<sup>33</sup> Other systems utilize implantable enzyme-based biofuel cells that are able to generate power from substances such as glucose and oxygen found in the host's body.<sup>34</sup> There are significant practical constraints on the amount of power that can be obtained from such sources.

Other neuroprosthetic devices may be passive devices that rely on the activity of the host's natural neurons or other biological structures or systems to control and manipulate the device and which thus do not need their own power source. Some kinds of nanorobot swarms may be able to draw power from chemicals found (naturally or through artificial addition) within the bloodstream of their human host. Other devices may be able to receive electricity provided wirelessly, e.g., through radio frequency induction.<sup>35</sup> Other devices may require periodic recharging through connection of a physical power cable to an external power port, permanent connection of such a cable, or the periodic replacement of a battery by means of some cover or port that is accessible either on the surface of the host's body or through an invasive surgical procedure.

### Emergency shutoff<sup>36</sup>

---

<sup>32</sup> NIST SP 800-53, Rev. 4 (2013), p. F-133.

<sup>33</sup> See Mitcheson, “Energy harvesting for human wearable and implantable bio-sensors” (2010).

<sup>34</sup> See Zebda et al., “Single glucose biofuel cells implanted in rats power electronic devices” (2013), and MacVitte et al., “From ‘cyborg’ lobsters to a pacemaker powered by implantable biofuel cells” (2013).

<sup>35</sup> See Borton et al., “Implantable Wireless Cortical Recording Device for Primates” (2009).

<sup>36</sup> NIST SP 800-53, Rev. 4 (2013), p. F-133.

For many kinds of general-purpose computers used within organizations, the recommended best practice is for the computer to include an emergency shutoff switch that can be easily accessed and used by authorized personnel, should the need arise – but which cannot be accessed or used by unauthorized parties. In the case of advanced neuroprosthetic devices, a number of factors will influence whether a particular device should include a physical emergency shutoff switch and, if such a shutoff switch does exist, who will have access and authorization to use it. In some cases, the presence and use of a physical emergency shutoff switch that can shut off power to a neuroprosthetic device could cause permanent physical or psychological harm to the device's host or to others; in other cases, the presence and use of such a shutoff switch may be needed precisely in order to prevent such harm. In some cases, it is essential that the host of a neuroprosthetic device have access to such a shutoff switch (because he or she will be best positioned to know when it should be used and to physically activate it), while – insofar as possible – other persons in the host's vicinity should be prevented from knowing about the shutoff switch's existence or being able to access and use it. In other cases, the kind of emergency situations that would require immediate use of the shutoff switch would also render the device's human host physically or psychologically incapable of utilizing the switch; in these cases, the shutoff switch should be physically accessible to bystanders and other persons, and it may even be desirable to install a light or audible alarm or other system to catch the attention of emergency medical personnel or other bystanders in situations that call for the use of the shutoff switch.<sup>37</sup>

### Emergency power<sup>38</sup>

For some kinds of neuroprosthetic devices, it may be possible and desirable to utilize an emergency power system (such as one which requires that an external power cable be plugged into a visible external port or jack in the neuroprosthetic device) that would not be practical in non-emergency situations, when the device's host expects to be able to move freely at will between different environments without the need to be plugged into a fixed power source. Small internal batteries may also be able to provide emergency power for a limited period of time, even though they would be inadequate for powering the device for sufficiently long periods during everyday non-emergency use.

---

<sup>37</sup> See Chapter Three of this text for a discussion of emergency access to implanted neuroprosthetic devices and, in particular, the possible use of subcutaneous buttons.

<sup>38</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-134.

## Fire protection<sup>39</sup>

Although it may not be possible to build full fire-suppression systems directly into neuroprosthetic devices, some devices that are composed of flammable materials or whose operation has the potential to generate excessive heat or sparks may need to at least include built-in fire-detection systems, with the device's host or operators maintaining external fire-suppression systems that are always available for use in emergencies.

## Temperature and humidity controls<sup>40</sup>

It may be crucial to implement systems that maintain a neuroprosthetic device within a predetermined range of temperatures and which ensure that other internal and external environmental conditions are maintained – not only to ensure that the device remains within appropriate operating parameters but that surrounding biological tissue and processes (which may be sensitive to even minute temperature changes) are not damaged by excessive heat or other emissions from the unit.

## Location of information system components<sup>41</sup>

General best practices include choosing – insofar as is feasible – to house information system components in a location that is protected against “flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation” and which lacks “physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).”<sup>42</sup> In the case of advanced neuroprosthetic devices, the fact that a device's human host is potentially able to take a device anywhere in the world may make it difficult or impossible to prevent a device from being brought into areas exposed to such situations – a danger that is present for mobile devices more generally.

## Information leakage<sup>43</sup>

---

<sup>39</sup> NIST SP 800-53, Rev. 4 (2013), p. F-135.

<sup>40</sup> NIST SP 800-53, Rev. 4 (2013), p. F-135.

<sup>41</sup> NIST SP 800-53, Rev. 4 (2013), p. F-137.

<sup>42</sup> NIST SP 800-53, Rev. 4 (2013), p. F-137.

<sup>43</sup> NIST SP 800-53, Rev. 4 (2013), p. F-138.

A neuroprosthetic device should be protected against “the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations.”<sup>44</sup> This may be especially difficult when multiple devices within a single body form a body area network (BAN) or body sensor network (BSN) whose components communicate with one another through wireless signals; the use of components that transmit signals through bodily tissue using means that do not broadcast signals into the atmosphere may reduce that risk.

The danger of information leakage may also be relatively high in the case of a neuroprosthetic device implanted within the interior of its host’s body that possesses no physical port or socket accessible on the external surface of the body and which must communicate with external diagnostic, control, or support systems utilizing wireless means.

### Asset monitoring and tracking<sup>45</sup>

Monitoring and tracking the location of an implanted neuroprosthetic device raises complex legal and ethical questions, insofar as this necessarily entails monitoring and tracking the location of the human host in whom it is implanted.<sup>46</sup>

## Contingency planning

### Contingency plan<sup>47</sup>

The development of effective contingency plans for advanced neuroprosthetic devices is essential, insofar as a failure or disruption in service with some devices may result instantaneously in life-threatening harm for the device’s human host or others. A contingency plan may contain procedures for continuing or resuming either all or some of a device’s functions and preserving critical assets in the face of various disruptions – if not through the device itself then through other available systems.

---

<sup>44</sup> NIST SP 800-53, Rev. 4 (2013), p. F-138.

<sup>45</sup> NIST SP 800-53, Rev. 4 (2013), p. F-138.

<sup>46</sup> This and related issues are discussed in Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants” (2012); McGee, “Bioelectronics and Implanted Devices” (2008); Mak, “Ethical Values for E-Society: Information, Security and Privacy” (2010); McGrath & Scanail, “Regulations and Standards: Considerations for Sensor Technologies” (2013); and Shoniregun et al., “Introduction to E-Healthcare Information Security” (2010).

<sup>47</sup> NIST SP 800-53, Rev. 4 (2013), p. F-78.

### Contingency training<sup>48</sup>

Contingency training may be especially important for a device's human host if the failure or disruption of the device's service will leave the host with only a limited window of time in which to carry out critical remedial actions before the service failure leaves the host incapacitated and unable to carry out such actions.

### Contingency plan testing<sup>49</sup>

Some kinds of contingency plan testing (such as the use of walk-throughs and checklists) may be easy to carry out, however an accurate full-scale simulation of some kinds of contingencies may be difficult to perform insofar as they would require simulating certain kinds of mental phenomena or incapacities on the part of the human host and the impact that these would have on the host, and replicating such conditions cannot be accomplished without causing actual harm to the host.

### Alternate storage site<sup>50</sup>

The use of an alternate storage site external to the body of a device's human host for storing information generated by an implanted neuroprosthetic device may not be possible for some devices that store information in particular kinds of systems (such as a physical neural network<sup>51</sup>) or which lack an adequate means of transmitting the relevant quantity and type of information to external systems.

### Alternate processing site<sup>52</sup>

The use of alternate processing sites for the processing of information by a neuroprosthetic system may not be possible if the act of processing is in part performed by the neurons within the host's brain or other biological systems within the host's body or if processing can only be carried out by the device when it enjoys a direct physical interface with the host's brain or body.

### Telecommunications services<sup>53</sup>

---

<sup>48</sup> NIST SP 800-53, Rev. 4 (2013), p. F-81.

<sup>49</sup> NIST SP 800-53, Rev. 4 (2013), p. F-82.

<sup>50</sup> NIST SP 800-53, Rev. 4 (2013), p. F-83.

<sup>51</sup> See the device ontology in Chapter Four of this text for a discussion of the structure and mechanics of such systems that include or comprise physical artificial neural networks.

<sup>52</sup> NIST SP 800-53, Rev. 4 (2013), p. F-83-F-84.

<sup>53</sup> NIST SP 800-53, Rev. 4 (2013), p. F-85.

A neuroprosthetic device may or may not be capable of using general-purpose communications technologies and services as a backup system if the device's own telecommunications system (which may be proprietary or demonstrate unique specifications for its speed, capacity, and format) were to fail or be disrupted.

### Information system backup<sup>54</sup>

For some kinds of advanced neuroprosthetics (such as those utilizing a complex physical neural network and holonomic storage system) it may be impossible to create a coherent backup, insofar as this would require taking a “snapshot” of the entire constantly-changing system at a single instant, but the processes available for detecting and recording the state of information within the system's components can only scan components sequentially and requires a long period of time to complete a single full scan of the system.<sup>55</sup>

### Information system recovery and reconstitution<sup>56</sup>

In the case of some kinds of neuroprosthetics (e.g., those utilizing a complex physical neural network), it may theoretically be possible to scan and record the state of the entire system at a single moment in time – thus creating a backup file – however there may be no mechanism available for restoring the system to a previous state by overwriting the device's current state with the information contained in the backup file.

### Safe mode<sup>57</sup>

For some kinds of neuroprosthetic devices it may be desirable to develop a safe mode with a predefined and limited set of features and operations that can either be manually activated by the device's operator or human host, if it becomes apparent that the host is entering (or about to enter) some situation in which unrestricted operation of the device would be hazardous to the host or others or which will be automatically activated if the device detects that

---

<sup>54</sup> NIST SP 800-53, Rev. 4 (2013), p. F-87.

<sup>55</sup> Regarding related technologies that have been proposed by some transhumanists as a possible path toward “mind uploading,” see Koene, “Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation” (2012); Proudfoot, “Software Immortals: Science or Faith?” (2012); Pearce, “The Biointelligence Explosion” (2012); Hanson, “If uploads come first: The crack of a future dawn” (1994); and Moravec, *Mind Children: The Future of Robot and Human Intelligence* (1990).

<sup>56</sup> NIST SP 800-53, Rev. 4 (2013), p. F-87-F-88.

<sup>57</sup> NIST SP 800-53, Rev. 4 (2013), p. F-89.

certain conditions are met.<sup>58</sup> Note that if activating the device's safe mode will result in a loss of consciousness or in some other impairment for the device's host, then the device may also need to possess a mechanism for determining when to automatically exit safe mode and resume normal operations, insofar as the host would not be able to manually initiate such an action.

### Alternative security mechanisms<sup>59</sup>

A neuroprosthetic device may possess backup security controls (e.g., alternate methods for user authentication) that become active only if the device's primary controls have been compromised.

## Configuration management

### Baseline configuration<sup>60</sup>

It may be difficult or impossible to specify a baseline configuration for some kinds of advanced neuroprosthetic devices, such as a mnemocybernetic device consisting of a physical artificial neural network that is integrated at the neural level with natural neurons in the host's brain and which does not have a set of discrete settings that can be centrally updated and applied to all individual neurons throughout the system after it has been activated. It may be impossible to intentionally roll back such a device to a previous configuration (or even to identify what such a configuration might be).

### Configuration change control<sup>61</sup>

Some neuroprosthetic devices may possess a configuration that is continuously altered in automatic response to stimulation and other activity by the host's biological systems with which it is integrated, without any means for the operator to directly control the configuration changes.

### Security impact analysis<sup>62</sup>

For some neuroprosthetic devices it may not be possible to fully analyze the security impact of potential configuration changes prior to actually implementing the changes, if the device's exact response to the changes depends

---

<sup>58</sup> Regarding the possibility that an IMD could detect when, e.g., a medical emergency is being experienced by its human host, see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010), pp. 921-22. See Chapter Three of this text for a broader discussion of failure modes for neuroprosthetic devices during emergency situations.

<sup>59</sup> NIST SP 800-53, Rev. 4 (2013), p. F-89.

<sup>60</sup> NIST SP 800-53, Rev. 4 (2013), p. F-64.

<sup>61</sup> NIST SP 800-53, Rev. 4 (2013), p. F-66.

<sup>62</sup> NIST SP 800-53, Rev. 4 (2013), p. F-68.



on the action of biological or psychological processes within the device's human host that cannot be simulated in a virtual test environment.

### **Least functionality<sup>63</sup>**

In the case of a neuroprosthetic system that is designed primarily to provide some necessary medical service or functional enhancement to its human host rather than to secure particular information, there may be non-security reasons for the device to offer the greatest functionality possible rather than the least allowable.<sup>64</sup>

### **Information system component inventory<sup>65</sup>**

A neuroprosthetic system's operator should ideally keep an inventory of all devices in use that records each device's "manufacturer, device type, model, serial number, and physical location."<sup>66</sup> However, in the case of some neuroprosthetic devices (such as those grown or assembled from living biological material or comprising a swarm of countless nanorobots) it may be difficult to adequately capture the nature of a particular device using such descriptors, as each device may, in effect, be wholly unique and possess a form that is constantly shifting and evolving.<sup>67</sup>

### **Software usage restrictions<sup>68</sup>**

Software restrictions are often implemented to ensure that software is used in accordance with its licensing restrictions and to ensure that software such as a peer-to-peer file-sharing program is not used "for the unauthorized distribution, display, performance, or reproduction of copyrighted work."<sup>69</sup> In the case of neuroprosthetic systems, operators must be careful to ensure – for legal and ethical reasons – that any software restrictions that are capable of disabling or constraining the use of software products do not do so at a time or in a manner that could cause harm to the device's human host or others.

---

<sup>63</sup> NIST SP 800-53, Rev. 4 (2013), p. F-71-73.

<sup>64</sup> See Chapter Five of this text for a discussion of the trade-offs that sometimes occur between increased information security and increased functionality for neuroprosthetic devices.

<sup>65</sup> NIST SP 800-53, Rev. 4 (2013), p. F-73-F-74.

<sup>66</sup> NIST SP 800-53, Rev. 4 (2013), p. F-73.

<sup>67</sup> Such a possibility would raise challenges for use of the device ontology presented in Chapter Four of this text: in that case, the ontology would become a way of specifying a device's general structural and operational parameters rather than its exact current characteristics.

<sup>68</sup> NIST SP 800-53, Rev. 4 (2013), p. F-76.

<sup>69</sup> NIST SP 800-53, Rev. 4 (2013), p. F-76.

The policing of peer-to-peer file-sharing will also be complicated by the fact that in effect, the mind of a device's human host is a "peer-to-peer file-sharing program" that is frequently exchanging information of all kinds with other human beings. Complex legal questions may also arise surrounding what constitutes a "display or performance" of copyrighted material: for example, in the past, using a hidden video camera to videotape a movie that was being shown in a commercial cinema and then uploading the bootleg video to a video-streaming site on the Internet would have been considered an illicit use of copyrighted material, but observing the film carefully with one's natural eyes, storing that sensory record in one's natural memory systems, and later using one's voice to describe the film to one's friends would not have been considered an illicit act. Such boundaries between licit and illicit usage may become blurred, for example, if one possesses artificial eyes or a mnemoprosthetic device that allow one to record *all* of one's daily visual experience – and not simply a film in a cinema – with high resolution and perfect fidelity or if one possesses an artificial voicebox that allows one not simply to speak with one's "own" natural voice but to play back any recorded sounds, including those that one may have overheard during a film screening.<sup>70</sup>

Complex questions – to be resolved by law, regulation, or individual licensing agreements – will also arise regarding intellectual property that is created with the aid or participation of a neuroprosthetic device. If a human host utilizes a device that enhances his or her memory, imagination, or artistic, mathematical, physical, or reasoning abilities, then any literary or artistic works, performances, inventions, or discoveries developed by the host may ultimately be the property of the neuroprosthetic device's manufacturer, provider, app developer, operator, or human host, or it may be owned jointly by some combination of parties.

### User-installed software<sup>71</sup>

Blocking the installation of software to a neuroprosthetic device by its user may or may not be legally and ethically permissible, as in some situations this may be equivalent to blocking a human being from adding thoughts, memories, or other permissible content to his or her own mind.

---

<sup>70</sup> For the notion that a neuroprosthetic device could be used for sensory recording or playback, see Merkel et al., "Central Neural Prostheses" (2007); Robinett, "The consequences of fully understanding the brain" (2002); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>71</sup> NIST SP 800-53, Rev. 4 (2013), p. F-76-F-77.

## Maintenance

### Controlled maintenance<sup>72</sup>

Conducting maintenance procedures on an advanced neuroprosthetic may require performing a surgical operation on the device's host, which would necessitate close coordination with the host and medical personnel. Even in cases when no surgical procedures are required, maintenance operations should be planned and scheduled in such a way that they do not cause undue interruption or impairment to the host's physical and cognitive capacities and, in particular, that they do not cause physical or psychological harm to the host or others. Conducting all maintenance within a secure facility may be desirable in order to ensure, for example, that automated maintenance instructions that are sent remotely to the neuroprosthetic device and which will result in a temporary device outage or change in the unit's functionality do not arrive when the device's host is engaged in performing a critical or potentially dangerous task.<sup>73</sup>

### Maintenance tools<sup>74</sup>

Standard practices which prevent the unauthorized removal of system maintenance software or tools from a device and which restrict their use may not be appropriate for neuroprosthetic systems that are a part of their host's organism; legal and ethical considerations may dictate that the host have full access to maintenance tools, including the ability to remove them. Emergency medical personnel treating the host may also need immediate unfettered access to some system maintenance tools that will allow them to affect or control a device's current operations, even if they are not provided full (or even partial) access to information stored within the device.<sup>75</sup>

### Maintenance personnel<sup>76</sup>

Efforts by a neuroprosthetic device's operator to limit who is allowed to conduct maintenance activities on the device – thereby restricting the host's ability to select his or her own maintenance personnel may not be legal or

---

<sup>72</sup> NIST SP 800-53, Rev. 4 (2013), p. F-112.

<sup>73</sup> Regarding different possible service outage or maintenance schedules and their impact on a neuroprosthetic device's availability, see Chapter Three of this text.

<sup>74</sup> NIST SP 800-53, Rev. 4 (2013), p. F-113-F-114.

<sup>75</sup> See Chapter Three of this text for a discussion of different approaches to providing medical personnel with emergency access to a neuroprosthetic device.

<sup>76</sup> NIST SP 800-53, Rev. 4 (2013), p. F-116.

ethical, given the device's status as an implantable device that may be considered an integral part of the host's body.

Given the extremely large financial commitment that may be involved with acquiring authorized replacement parts and maintenance services for some kinds of neuroprosthetic devices, there may be strong financial incentives for the human hosts (or potentially operators) of neuroprosthetic devices to seek out replacement components and services through less-expensive unauthorized black- or gray-market channels offering pirated or counterfeit components and services that are lacking quality guarantees or warranties and are provided by individuals lacking formal training, licensing, or insurance. Such unauthorized channels may sometimes offer products that are more expensive than their authorized counterparts because they are free from standard security or DRM mechanisms or have been legally banned or offer services that cannot legally be provided or received.<sup>77</sup>

## Timely maintenance

### **PREDICTIVE MAINTENANCE**<sup>78</sup>

Efforts to require the host of a neuroprosthetic device to submit to mandatory preventative maintenance on the device on the basis of predictive algorithms, a fixed calendar, or an *ad hoc* decision on the part of the device's operator may or may not be legal, if the maintenance may impact the host's physical or cognitive functioning and he or she does not wish to submit to it.

## System and information integrity

### Flaw remediation

### **CENTRAL MANAGEMENT**<sup>79</sup>

Some kinds of "flaws" detected in the functioning or operation of a neuroprosthetic device may be flaws not in the physical device or its software but in the structure and behavior of the larger device-host system in which it participates; in such circumstances, detection and remediation of the flaw may depend largely on the individual capacities and action of the device's human host rather than the organizations responsible for designing, manufacturing, providing, or operating such neuroprosthetic devices.<sup>80</sup>

---

<sup>77</sup> For the possibility of hosts modifying their own devices in unanticipated and potentially unwise and illicit ways, see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010).

<sup>78</sup> NIST SP 800-53, Rev. 4 (2013), p. F-118.

<sup>79</sup> NIST SP 800-53, Rev. 4 (2013), p. F-216.

<sup>80</sup> See Chapter Three of this text for a discussion of the distinction between a neuroprosthetic

**TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTION<sup>81</sup>**

In the case of some kinds of neuroprosthetic devices that interact with or support biological processes critical to the health of their human hosts, both legal, ethical, and operational considerations may dictate that a flaw must be corrected immediately upon its detection; the fact that an organization works “as quickly as possible” to resolve the problem may not absolve it of responsibility for damage that occurs as a result. This is especially true in the case of devices that cannot easily be recalled, removed, or replaced if a flaw is discovered after a device has been implanted in its human host.<sup>82</sup>

**AUTOMATIC SOFTWARE/FIRMWARE UPDATES<sup>83</sup>**

Allowing the automatic downloading, installation, and execution of operating system or application updates by neuroprosthetic devices should only be undertaken after careful consideration, especially for devices with critical health impacts for their human hosts. The fact that operating system or application updates have undergone beta testing in a simulated development environment or with a limited number of host-device systems prior to their widespread public release may not ensure that the updates will not cause severe and unexpected negative impacts on the functioning of some implanted neuroprosthetic devices and harm for their human hosts, given the fact that the functioning of individual neuroprosthetic devices may vary greatly depending on the unique nature of each device’s physical interface with the neural circuitry of its human host and the nature of the host’s cognitive patterns and activity.

## Malicious code protection

**TESTING/VERIFICATION<sup>84</sup>**

A neuroprosthetic device’s mechanisms for protecting the device and device-host system against malicious code can be tested “by introducing a known benign, non-spreading test case into the information system.”<sup>85</sup> Great care should be taken and all legal, ethical, and practical implications considered before intentionally introducing such code into a neuroprosthetic device

---

device and its device-host system.

<sup>81</sup> NIST SP 800-53, Rev. 4 (2013), p. F-216.

<sup>82</sup> See Chapter Three of this text for a discussion of how the concept of zero-day vulnerabilities and attacks relates to neuroprosthetic devices – and especially to those possessing critical health impacts for their human host.

<sup>83</sup> NIST SP 800-53, Rev. 4 (2013), p. F-216.

<sup>84</sup> NIST SP 800-53, Rev. 4 (2013), p. F-218.

<sup>85</sup> NIST SP 800-53, Rev. 4 (2013), p. F-218.

that is already integrated into the neural circuitry of a human host, as code that had previously been believed to be “benign” and “non-spreading” when studied in a laboratory setting may behave in unpredictable ways when exposed to or affected by the unique biological structures or activity of a particular human host.

#### **NONSIGNATURE-BASED DETECTION<sup>86</sup>**

Heuristic analysis and other approaches or mechanisms can be used to identify malicious code that is polymorphic or metamorphic and which cannot be identified by antivirus software that searches for particular known signatures. In the case of some kinds of neuroprosthetic devices (e.g., those that utilize certain types of physical neural networks and do not execute programs as traditionally understood), malicious “code” may not take the form of discrete strings of digital information that can be analyzed to detect particular signatures but may instead take the form of sense data or other forms of environmental phenomena that can affect a neuroprosthetic device or device-host system. In such situations, the use of heuristic analysis and probabilistic methods to identify potentially malicious input may be necessary.<sup>87</sup>

#### **DETECT UNAUTHORIZED COMMANDS<sup>88</sup>**

Information systems are often designed to detect unauthorized operating system commands at the level of the kernel application programming interface, block the execution of such commands, and issue an alert regarding the commands.<sup>89</sup> Such mechanisms are important not just for preventing certain kinds of attacks purposefully launched against information systems by adversaries but also for preventing unauthorized commands that may be an unintentional result of some hardware or software failure, quantum-level metastability, or other phenomenon. Guarding against the execution of unauthorized commands is especially important in the case of neuroprosthetic devices with critical health impacts for their human host.

#### **AUTHENTICATE REMOTE COMMANDS<sup>90</sup>**

It is especially important for a neuroprosthetic device to properly authenticate remote commands in cases in which the device receives instructions

---

<sup>86</sup> NIST SP 800-53, Rev. 4 (2013), p. F-218.

<sup>87</sup> For some such neuroprosthetic systems, the process of detecting a malicious vector may be less like that of detecting a traditional computer virus (e.g., a kind of binary data file) and more like that of identifying a potentially malicious *person*, a potentially damaging social relationship, or a potentially harmful sensory experience.

<sup>88</sup> NIST SP 800-53, Rev. 4 (2013), p. F-218.

<sup>89</sup> NIST SP 800-53, Rev. 4 (2013), p. F-218.

<sup>90</sup> NIST SP 800-53, Rev. 4 (2013), p. F-219.

from external medical control or support systems that can affect or control the device's impact on critical health functions of its human host.

### **MALICIOUS CODE ANALYSIS<sup>91</sup>**

In the case of neuroprosthetic devices that utilize biological components or materials, “malicious code” may potentially take the form of genetic sequences delivered through the use of biological (and not computer) viruses, microorganisms, or other biological vectors. A sophisticated attack on such a neuroprosthetic device might combine both the use of a computer virus or worm that infects and compromises electronic portions of the device and a biological vector that infects and compromises the biological portions of the device. In the case of a neuroprosthetic device that controls, supports, or executes the production of hormones, cells, or other biochemical products within the host's body, a computer worm or virus or attack that compromises the electronic portion of the device could conceivably be used to generate biochemical agents that would in turn infect and compromise biological components of the neuroprosthetic device or of the host's natural organism. Conversely, a biological vector or biochemical agent that infects biological components of the host's organism or of a neuroprosthetic device could conceivably be used to introduce a computer virus or worm into the device's electronic components, if the device's electronic components receive and process information or other input from biological or biochemical components or systems within the host's organism or the neuroprosthetic device.

### **Information system monitoring<sup>92</sup>**

Significant legal, ethical, and practical questions arise regarding an organization's deployment of monitoring devices to monitor an organizational information system. Although such monitoring may have the legitimate purpose of detecting or dissuading attacks, it may sometimes also gather personal information on the activities, health, and other characteristics of organizational members or outside parties in ways that is legally and ethically impermissible. External systems (e.g., medical imaging or diagnostic equipment) may be used to monitor the activities of a neuroprosthetic device or device-host system. Alternatively, a neuroprosthetic device may itself be used by an organization as a monitoring device to monitor the activity of other conventional information systems belonging to the organization (e.g., servers or desktop computers). Other implantable components within the same host

---

<sup>91</sup> NIST SP 800-53, Rev. 4 (2013), p. F-219.

<sup>92</sup> NIST SP 800-53, Rev. 4 (2013), p. F-219-F-220.

as a neuroprosthetic device may be used to monitor the activities of the device and device-host system.<sup>93</sup>

#### **SYSTEM-WIDE INTRUSION DETECTION SYSTEM<sup>94</sup>**

Intrusions *into* neuroprosthetic devices may be detected by standard tools that monitor the electronic components and systems of the device; they may also be potentially be detected as alterations in the device's functioning by the human host with whose neural circuitry a device is integrated. Intrusions into conventional information systems committed *using* neuroprosthetic devices may – depending on the nature of the intrusion – be detected by traditional intrusion-detection mechanisms, be detected by specialized detection mechanisms designed specifically to recognize the presence and activity of neuroprosthetic devices, or be difficult to detect by any means.<sup>95</sup>

#### **ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES<sup>96</sup>**

In the case of general-purpose organizational information systems, anomalous communications traffic may include “large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.”<sup>97</sup>

In the case of advanced neuroprosthetic devices, anomalous traffic at the external boundaries of the system may result from unusually intense or numerous environmental stimuli impacting a sensory neuroprosthetic (perhaps reaching the level of sensory overload), unusually intense or complex motor instructions being sent to motor organs (e.g., when attempting to speak, play a musical instrument, or engage in sports activities), or unusually intense, rich, or complex cognitive activities (e.g., caused by or reflected in heightened emotion, a state of dreaming or hallucination, or the act of imagining new ideas or retrieving old memories). Note that activities which may produce “anomalous” communications traffic patterns when viewed in relation to a neuroprosthetic device may be quite commonplace from the perspective of a device's human host.

---

<sup>93</sup> For a discussion of ethical and legal aspects relating to such issues, see Kosta & Bowman, “Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants” (2012); McGee, “Bioelectronics and Implanted Devices” (2008); Mak, “Ethical Values for E-Society: Information, Security and Privacy” (2010); McGrath & Scanail, “Regulations and Standards: Considerations for Sensor Technologies” (2013); Shoniregun et al., “Introduction to E-Healthcare Information Security” (2010); and Brey, “Ethical Aspects of Information Security and Privacy” (2007).

<sup>94</sup> NIST SP 800-53, Rev. 4 (2013), p. F-220.

<sup>95</sup> See Chapter Three of this text for a discussion of neuroprosthetic devices as potential tools for use in launching cyberattacks or other kinds of attacks.

<sup>96</sup> NIST SP 800-53, Rev. 4 (2013), p. F-221.

<sup>97</sup> NIST SP 800-53, Rev. 4 (2013), p. F-221.



**WIRELESS INTRUSION DETECTION<sup>98</sup>**

Organizations may use a wireless intrusion detection system to scan for and detect both the connection of unauthorized wireless devices to the organization's own wireless access points as well as the presence of unauthorized wireless access points within organizational facilities.<sup>99</sup> Such wireless intrusion detection systems may be used, for example, to identify visitors to organizational facilities who are using nonvisible neuroprosthetic devices to make unauthorized connections to organizational information systems or to identify miniaturized neuroprosthetic devices that may have been implanted in organizational personnel without their knowledge and which are attempting to wirelessly contact command-and-control servers for instructions or to transmit gathered intelligence.<sup>100</sup>

**CORRELATE MONITORING INFORMATION<sup>101</sup>**

Given the resources needed for transmitting, receiving, and processing all of the monitoring data from a wide array of sources that is to be correlated, such correlation may often be handled best by external systems that are managed by the operators of a neuroprosthetic device. The use of an external system that is housed within a conventional information systems facility avoids the severe limitations on memory storage, communications bandwidth, and processing capacity that affect many implantable neuroprosthetic devices due to their great size, power, and operational constraints. Particular insights, conclusions, or instructions that result from the correlation of monitoring information in an external system can then be conveyed to a device or to the device's host or operator for use as appropriate.

**INTEGRATED SITUATIONAL AWARENESS<sup>102</sup>**

Organizations integrate information obtained "from a combination of physical, cyber, and supply chain monitoring activities"<sup>103</sup> in order to better detect cyberattacks (which may be complex and multifaceted operations that have both physical and virtual components and which target both an employer's operation of a neuroprosthetic device and the suppliers who de-

---

<sup>98</sup> NIST SP 800-53, Rev. 4 (2013), p. F-222.

<sup>99</sup> NIST SP 800-53, Rev. 4 (2013), p. F-222.

<sup>100</sup> See Chapter Three of this text for a discussion of the reliance on wireless communication found with many kinds of neuroprosthetic devices.

<sup>101</sup> NIST SP 800-53, Rev. 4 (2013), p. F-222.

<sup>102</sup> NIST SP 800-53, Rev. 4 (2013), p. F-222.

<sup>103</sup> NIST SP 800-53, Rev. 4 (2013), p. F-222.

signed and produced the physical components and software used in the device). For individual human hosts who operate neuroprosthetic devices that they have purchased or leased as consumer electronics devices, developing such integrated situational awareness relating to their devices can be difficult. For such an individual, the physical monitoring of his or her device may be relatively easy, insofar as the device is always physically present with the host, and in order for unauthorized parties to physically access the device they may need to physically access or manipulate the host's biological body. Awareness of cyberattacks or other unauthorized access may be more difficult for the host to achieve and may depend on a combination of effective security controls built into the device, its OS, and its applications, as well as personal knowledge of and commitment to information security best practices on the part of the device's host. Full supply chain monitoring may be difficult or impossible for the host to carry out: although he or she may know the identity of the organizations that were responsible for assembling and distributing the finished physical device and distributing its operating system and installed applications, it may be difficult for the host to determine who designed and manufactured individual components within the device, and who may have served as a subcontractor writing and testing outsourced portions of the operating system and applications on behalf of the primary developer. In the case of open-source software, it may be more difficult to know exactly the true identity of the parties responsible for providing particular elements of code, but it may simultaneously be easier to scrutinize the contents of code themselves.

#### **ANALYZE TRAFFIC / COVERT EXFILTRATION**<sup>104</sup>

The analysis of traffic to detect and prevent covert exfiltration may be desirable and necessary even in the case of neuroprosthetic devices whose actions are clearly visible to their human host and which are theoretically engineered to transmit information or perform actions only in accordance with the volition of their human host. For example, an advanced neuroprosthetic arm may be controlled by motor impulses originating in the host's brain, and its movements are visible to the eyes of its human host. However, a computer virus or adversary's cyberattack that is able to compromise the device and alter the motor instructions received by the device from the host's brain (or fabricate nonexistent motor instructions) may be able to cause the neuroprosthetic arm to move in minute ways or with subtly altered patterns that are undetectable to the host's natural biological eyes and visual perception but which can be detected and interpreted by adversarial systems and used

---

<sup>104</sup> NIST SP 800-53, Rev. 4 (2013), p. F-222.

to exfiltrate information from the device or device-host system.<sup>105</sup> In a sense, such a case would represent a form of **cognitive steganography** or **motor steganography**.

#### **PROBATIONARY PERIODS<sup>106</sup>**

The use of probationary periods for individuals receiving authorized access to information systems may not be legally, ethically, or practically feasible to employ in the case of hosts in whom neuroprosthetic devices are being implanted. Any “probationary period” designed to ensure a host’s knowledge of and commitment to organizational policies (including information security practices) may need to take place before the device is implanted and integrated into the host’s neural circuitry, as it could be impossible to remove or deactivate the device after its implantation if the host should not successfully complete the probationary period. On the other hand, any probationary period designed to test the host’s ability to successfully operate a device and use it to perform necessary information security tasks may necessarily need to take place after the device has been implanted (and after the host has undergone any required recovery, adaptation, and training period), as it may be impossible to simulate operational conditions or fully train and test the host in the device’s use prior to the device’s physical integration with the host’s neural circuitry.

#### **HOST-BASED DEVICES<sup>107</sup>**

In the sense used here, the word “host” does not refer to the human being in whom a neuroprosthetic device is physically implanted but to the device (such as a server or desktop computer) that serves as a host in a host-client device system. In the case of an organization that has deployed many neuroprosthetic devices among its personnel, the organization may operate a centralized information system housed within a secure organizational facility that serves as the host for the client neuroprosthetic devices. If all of the client devices are monitored or controlled by, receive software updates from, or are otherwise affected by the centralized system, the use of effective security controls to protect that central system is important for securing its client devices.

---

<sup>105</sup> Regarding the possibility that a neuroprosthetic limb could be hacked or otherwise compromised by an adversary and that its behavior could be remotely controlled or manipulated, see Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

<sup>106</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-223.

<sup>107</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-223.

**INDICATORS OF COMPROMISE<sup>108</sup>**

Organizations may use automated or manual procedures for searching for indicators of compromise (IOCs), which are detectable traces created or left within an information system that may indicate that the system has been compromised; such IOCs may include new registry key values or records of network traffic between the system and known command-and-control servers.<sup>109</sup> In the case of advanced neuroprosthetic devices, IOCs may potentially take radically new and different forms, such as the presence of unexplained or corrupted memories or memory fragments within the mind of the device's host, the host's display of unusual sensory, motor, emotional, or personality-related behaviors, or the presence of particular hormones, other chemicals, or other objects within the host's bloodstream or body.<sup>110</sup>

**Security alerts, advisories, and directives<sup>111</sup>**

In the case of some kinds of sensory or cognitive neuroprosthetics, it may be possible for an organization to deliver a security alert or directive instantaneously and directly to the conscious awareness of a device's host through sensory input or augmented reality. However, if such methods are used by an organization as the primary or only way of delivering such alerts and directives, care must be taken to ensure that this delivery system cannot be blocked, disrupted, or manipulated by an adversary in order to facilitate a cyberattack on the device's host.

**Security function verification<sup>112</sup>**

In addition to regular ongoing security function verification, it is important to conduct special verification when a system is undergoing transitional states such as being powered on, rebooted, or shut down.<sup>113</sup> For some kinds of neuroprosthetic devices, key transitional states may also relate to the sensory, cognitive, and motor processes displayed by device's human host, such as entering or leaving sleep, opening or closing eyelids, or initiating gross motor movements.

**Software, firmware, and information integrity**


---

<sup>108</sup> NIST SP 800-53, Rev. 4 (2013), p. F-223.

<sup>109</sup> NIST SP 800-53, Rev. 4 (2013), p. F-223.

<sup>110</sup> For the possibility that an attack on a neuroprosthetic device or its device-host system might produce long-term changes in the neural activity or structures of the device's host, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

<sup>111</sup> NIST SP 800-53, Rev. 4 (2013), p. F-224.

<sup>112</sup> NIST SP 800-53, Rev. 4 (2013), p. F-224-F-225.

<sup>113</sup> NIST SP 800-53, Rev. 4 (2013), p. F-225.

**INTEGRITY CHECKS<sup>114</sup>**

Checking the integrity of a device's operating system or applications may be difficult or impossible in the case of some neuroprosthetic devices that utilize physical neural networks (and do not execute "programs" as conventionally understood) or which are passive devices that are directly controlled by the cognitive processes of their host's cognitive processes, which effectively provide the "operating system" for the device.<sup>115</sup> In the case of neuroprosthetic devices that utilize biological components for storing information and performing activities, it may be impossible to require the same level of integrity as that expected with electronic computers, insofar as the biological components may be undergoing gradual but continuous change through the birth, growth, mutation, and death of individual cells.

**AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS<sup>116</sup>**

Care must be taken that any automated responses to integrity violations detected within a neuroprosthetic device do not cause physical or psychological harm to the device's host or others. In some circumstances, automated responses may need to be delayed in order to prevent the device from malfunctioning or failing when it is being used by its host or operator to perform an urgent task (e.g., with potentially critical health impacts for the device's host). In other circumstances, an automated response may *need* to take place instantaneously in order to protect the device's host or operator from some critical health impact.

**INTEGRATION OF DETECTION AND RESPONSE<sup>117</sup>**

In the case of certain neuroprosthetic devices – for example, some utilizing a physical neural network that is broadly interconnected with the neural circuitry of the brain of the devices' host and whose operating system or applications are partly or wholly stored within the biological structures and cognitive processes of the host's brain – the detection of integrity violations and response to them may inherently be closely integrated, insofar as the same artificial neurons that receive input through their synthetic dendrites from natural neurons in the host's brain that allows the violation to be detected will also be involved in transmitting output through their synthetic axons to

---

<sup>114</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-225.

<sup>115</sup> See Chapter One of this text for a discussion of passive neuroprosthetic devices and Chapter Five for a discussion of integrity as an information security goal and attribute.

<sup>116</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-226.

<sup>117</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-226.

the connected natural neurons in an effort to remedy the violation of integrity.

#### **PROTECTION OF BOOT FIRMWARE<sup>118</sup>**

Some kinds of passive neuroprosthetic devices that are directly controlled by the “operating system” provided by the biological structures and processes of their host’s brain – as well as devices that include a physical neural network and whose functionality grows organically over time through learning and training – may not possess boot firmware as it is traditionally understood.<sup>119</sup>

#### **CODE EXECUTION IN CONFINED AND PROTECTED ENVIRONMENTS WITH LIMITED PRIVILEGES<sup>120</sup>**

Software whose source code is unavailable to an organization or which is suspected of containing malicious code is often installed and executed by an organization only within protected and physically or virtually isolated machines running with minimal privileges.<sup>121</sup> For some kinds of neuroprosthetic devices whose functionality and behavioral characteristics are inherently highly influenced by or dependent on the biological structures and biological or cognitive processes of their human host, it may not be possible to construct protected environments that fully replicate the functioning of such devices while remaining physically or virtually segregated from an actual human host. In such cases, software may need to be run within its live production environment, if it is to be run at all.

On the other hand, advanced neuroprosthetic devices may also create entirely new possibilities for constructing protected and physically or virtually isolated environments in which potentially malicious code can be run, insofar as they may allow InfoSec personnel possessing sensorimotor neuroprosthetics to create and interact with information systems in a virtual environment that is separated from physical organizational systems.

#### **BINARY OR MACHINE EXECUTABLE CODE<sup>122</sup>**

For some kinds of neuroprosthetic devices (e.g., those utilizing a physical neural network of biomimetic synthetic neurons) certain types of biochemical or electrochemical stimuli allowed to reach a device’s synthetic neurons could constitute a form of “machine executable code,” if the stimuli cause the neurons (or their connected systems) to respond by executing particular behaviors.

---

<sup>118</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-226-F-227.

<sup>119</sup> See Chapter One of this text for a discussion of passive neuroprosthetic devices of this sort.

<sup>120</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-227.

<sup>121</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-227.

<sup>122</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-227.

## Spam protection<sup>123</sup>

For individuals possessing advanced neuroprosthetic devices that edit or replace their natural sensory input to create an experience of augmented or virtual reality,<sup>124</sup> spam might come in the form of messages, advertisements, alerts, or any other kind of virtual audiovisual or other sensory phenomenon designed to elicit some behavior from a neuroprosthetic device's host. For individuals possessing some kinds of advanced cognitive neuroprosthetics, spam may potentially even take the form of memories, emotions, desires, beliefs, or other mental phenomena that are directly inserted into or created or altered within a host's cognitive processes by some external agent.

## CONTINUOUS LEARNING CAPABILITY<sup>125</sup>

Some kinds of neuroprosthetic devices may be able to utilize spam protection mechanisms that learn what is spam by directly detecting the physical or psychological reaction presented by a device's human host to incoming messages and stimuli, thereby supplementing or enhancing traditional learning mechanisms such as Bayesian filters that are often employed in spam protection systems.<sup>126</sup>

## Information input validation<sup>127</sup>

Information input validation is used to protect systems from being compromised through attacks that target the structured messages that are frequently used by an information system for communications between its different components or subsystems and which may include a combination of control information, metadata, and raw, unstructured contents.<sup>128</sup> If information input is not properly validated through adequate prescreening and filtering of raw input<sup>129</sup> from external systems or agents, it is possible that an adversary could supply carefully designed raw input to one component of a system that would then include the raw input in a structured message sent to a different component that may erroneously interpret the raw input as

---

<sup>123</sup> NIST SP 800-53, Rev. 4 (2013), p. F-228.

<sup>124</sup> For the possibility that a device that has been designed to receive raw data from the external environment could have that data supplemented or replaced by other data transmitted from some external information system, see Koops & Leenes, "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes" (2012).

<sup>125</sup> NIST SP 800-53, Rev. 4 (2013), p. F-228.

<sup>126</sup> NIST SP 800-53, Rev. 4 (2013), p. F-228.

<sup>127</sup> NIST SP 800-53, Rev. 4 (2013), p. F-229-F230.

<sup>128</sup> NIST SP 800-53, Rev. 4 (2013), p. F-229.

<sup>129</sup> NIST SP 800-53, Rev. 4 (2013), p. F-229.

though it were control information or metadata. With some kinds of sensory or cognitive neuroprosthetic devices, for example, there may exist a theoretical possibility that simply by presenting certain carefully crafted forms and patterns of stimulus in a way that they can be absorbed as raw input by a host's sensory organs (e.g., perhaps by generating a particular series of tones that can be detected by a host's natural ears or auditory neuroprosthetics, displaying certain text or symbols on a monitor viewed by the host's natural or artificial eyes, writing particular sequences of code as graffiti on the side of a building that the host will see, or uttering a particular string of words to the host in conversation), such raw input will be passed along to other components within the host's neuroprosthetic device or device-host system through a structured message in such a way that the raw input is interpreted as metadata or control information that will be executed or otherwise utilized by the neuroprosthetic device to generate some action or behavior desired by the adversary.<sup>130</sup>

In addition to the purely technical kind of information input validation needed to prevent such occurrences, the host or operator of a neuroprosthetic device may also potentially use such mechanisms for the prescreening and filtering of raw input (e.g., stimuli from the external environment detectable by sensory organs) to screen out particular kinds of content which the host or operator might find objectionable or undesirable for other reasons – whether for legal, ethical, cultural, or aesthetic reasons, or because the blocked or limited types of content have a negative operational impact on the functionality of the device or other biological or synthetic systems or processes within its host.

## Error handling<sup>131</sup>

Error messages generated by information systems should generally provide the kinds of information needed for organizational personnel to identify and remedy the source of the error without providing information that could be used by adversaries to either directly compromise the system or indirectly learn more about its functioning.<sup>132</sup> In the case of neuroprosthetic devices

---

<sup>130</sup> Hansen and Hansen discuss the hypothetical case of a poorly designed prosthetic eye whose internal computer can be disabled if the eye is presented with a particular pattern of flashing lights; see Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010). Although that example is of a different sort than the hypothetical cases just presented here (insofar as the case presented by Hansen and Hansen might conceivably involve a purely physical flaw or other vulnerability in the prosthetic eye that does not involve raw data being interpreted as structured data or metadata), it reflects the same basic notion that the functioning of a neuroprosthetic device could be disrupted or manipulated by providing the device with certain kinds of raw data.

<sup>131</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-230.

<sup>132</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-230.



with critical health impacts, error messages may need to be presented not only through internal sensory or cognitive processes to a device's host or through organizational information system's to the device's operator but potentially also to emergency medical personnel who previously had no connection to the host or the host's organization but who happened to be in the vicinity of a host, are diagnosing and treating him or her for some health emergency, and may not (yet) have full access to the neuroprosthetic device's components or processes.<sup>133</sup>

### Information handling and retention<sup>134</sup>

Individuals and organizations may be required to retain some information that is received, generated, stored, or transmitted by neuroprosthetic devices for legal, ethical, or practical reasons. Note that some kinds of neuroprosthetic devices that mimic or interface with the natural memory systems utilized by the human brain be store information in a way that is subject to significant compression, distortion, and degradation over time.<sup>135</sup> While storing information in our natural memory systems has, throughout human history, often been the best or only way of storing information, the use of neuroprosthetic devices that demonstrate such functional limitations may not be legally or ethically permissible in cases when more effective and reliable storage mechanisms are available.

### Predictable failure prevention<sup>136</sup>

A best practice is to determine the mean time to failure (MTTF) for information system components not simply by relying on reported industry aver-

---

<sup>133</sup> Chapter Three of this text considers many proposed technological approaches for granting emergency medical personnel access to a neuroprosthetic device in cases when its human host is experiencing a medical emergency. However, a perhaps understudied aspect of such situations is the fact that even if emergency medical personnel have the technological means by which to gain access to a particular neuroprosthetic device, this in no way guarantees that they will have the expertise in computer science, information technology, biomedical engineering, or cybernetics that may be required in order to quickly diagnose the device's status and functioning, alter its configuration, and perhaps even reprogram it in order to yield specific outcomes for and impacts on the host's biological organism.

<sup>134</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-230.

<sup>135</sup> Regarding questions surrounding the nature and quality of long-term memory storage in the human brain, see Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004).

<sup>136</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-231.

ages but by calculating the MTTF for components as they are used in particular installations, for example, by the organization.<sup>137</sup> Knowing the MTTF for components in use helps the organization to ensure that it has an adequate supply of replacement components on hand and is ready to repair or replace components when needed.

For some kinds of neuroprosthetic devices, the MTTF for individual components or the system as a whole may be influenced or determined by factors relating to the unique biological structures or processes of the devices' individual human hosts. In such cases, it may be impossible to accurately estimate the MTTF for components in a particular device until the device has been put into operation and components have begun to fail.

#### **STANDBY COMPONENT INSTALLATION/NOTIFICATION<sup>138</sup>**

Often the failure of a component triggers the automatic or manual transfer of the component's responsibilities to a standby component that was already in place and ready to be activated.<sup>139</sup>

In the case of implanted neuroprosthetic devices whose ability to communicate with external systems cannot be reliably guaranteed, whose functioning depends on direct physical access to biological structures or processes within their host's body, or which cannot be easily manually accessed for repair or replacement, it may not be possible to utilize standby components that are located externally to a host's body: any standby components may need to be implanted into a host's body at the same time as the primary neuroprosthetic device or may need to be directly incorporated into the structure of the primary neuroprosthetic device itself.

#### **FAILOVER CAPABILITY<sup>140</sup>**

The automatic switchover to an alternate system after the failure of an entire system typically requires that mirrored systems or alternate processing sites<sup>141</sup> have already been established and adequately prepared and maintained in advance of the moment when the failure occurs. If by "system" we understand an entire neuroprosthetic device (rather than individual components within it), the unexpected failure of such a system may cause significant physical or psychological harm to the device's host or operator, especially if the device has critical health impacts. In some cases, it may not be possible to install an alternate system at the same time as implantation of the primary

---

<sup>137</sup> NIST SP 800-53, Rev. 4 (2013), p. F-231. See Chapter Three of this text for a discussion of mean time to failure, mean time to repair, and availability for advanced neuroprosthetic devices.

<sup>138</sup> NIST SP 800-53, Rev. 4 (2013), p. F-231.

<sup>139</sup> NIST SP 800-53, Rev. 4 (2013), p. F-231.

<sup>140</sup> NIST SP 800-53, Rev. 4 (2013), p. F-231.

<sup>141</sup> NIST SP 800-53, Rev. 4 (2013), p. F-231.

neuroprosthetic device due to practical constraints such as space or power limitations or the fact that key biological structures and processes within the body of the primary device's host can interface with at most one device of that kind at a time.

In the case of “failure” of an entire device-host system (e.g., through the incapacitation or death of a device's human host), there may not be any possibility of failover to an alternate information system, insofar as it is not feasible to “mirror” such traits as the unique physical, legal, and ontological identity or continuity of consciousness and agency of a particular human being in a synthetic external information system, no matter how closely it may mimic some other traits displayed by the person (such as his or her genotype, physical appearance, or even the contents of his or her memory). While the concept of “uploading” key information relating to a human being into an information system or creating physical or virtual copies of key physical components or processes of the person has been proposed and much debated<sup>142</sup> – and such techniques could indeed be said to provide a limited “failover capability,” if the only goal is to preserve (partial and potentially inaccurate) records of some aspects of a human being's physical structure at a given point in time or of the person's past behavior – such mechanisms do not effect the continuation of a human being's essence or existence in any robust sense.

Perhaps the only way in which a neuroprosthetic device or neurocybernetic system could allow the continuation of the existence of a “human being” through failover to an alternate information system would be if the individual were not a natural biological human being to begin with (in the way that the expression is traditionally understood) but were rather a simulacrum that was already, in some sense, a copy or representation without an original.<sup>143</sup>

If the traditional understanding of the concept of a “human being” were someday to be expanded or transformed to such an extent (or simply replaced with a new understanding) so that an information system, virtual entity, software program, or instantiation of patterns within a neural network could be considered a “human being” simply because it displays certain human-like characteristics or contains information derived from human beings – without requiring that such information being housed within or accessed through a particular unique biological substrate – then it would be possible to imagine

---

<sup>142</sup> See Koene, “Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation” (2012); Proudfoot, “Software Immortals: Science or Faith?” (2012); Pearce, “The Biointelligence Explosion” (2012); Hanson, “If uploads come first: The crack of a future dawn” (1994); and Moravec, *Mind Children: The Future of Robot and Human Intelligence* (1990).

<sup>143</sup> See Baudrillard, *Simulacra and Simulation* (1994), for a discussion of such issues.

the preservation and continuation of an entire device-host system through failover to an entirely disjoint alternate system. However, such “preservation” or “continuation” is not at all the sort of preservation and continuation of personal consciousness, agency, and physical and noetic identity that a human being possessing a neuroprosthetic device would generally seek and which it may be the legal and ethical responsibility of the device’s operator to ensure.<sup>144</sup>

### Non-persistence<sup>145</sup>

Rather than waiting until it has been detected that particular components or services have been compromised and then replacing them, terminating their functionality, or otherwise addressing the situation, an organization may proactively refresh components and services at regular or random intervals.<sup>146</sup> Such procedures can reduce the effectiveness of certain kinds of **advanced persistent threats** (APTs) that must have access to or operate within a particular computing environment for a substantial period of time in order to successfully exploit vulnerabilities and complete their attack.<sup>147</sup> For some kinds of neuroprosthetic devices, non-persistence may be difficult to implement, insofar as a device must provide continual service and 100% availability in order to avoid causing physical or psychological harm for its host or operator, and the time and actions needed to refresh components or services would cause an impermissible interruption or disruption to the device’s functionality.<sup>148</sup> In other cases, it may be possible to refresh components or services during non-critical moments (e.g., when a device’s host is asleep or not engaging in particular kinds of activities). Other kinds of neuroprosthetic devices (e.g., those utilizing biological components or neural networks) may neither require nor allow such periodic refreshing of components or services.

### Information output filtering<sup>149</sup>

In the case of advanced motor neuroprosthetics, filtering may be used to (perhaps only temporarily) prevent the execution or expression of motor behavior that is identified as being anomalous and inconsistent with the kinds of motor behaviors expected from the device and the device-host system in

---

<sup>144</sup> See Proudfoot, “Software Immortals: Science or Faith?” (2012). See Chapter Three of this text for a discussion of the need to protect the personal identity, autonomy, agency, and sapient awareness of a neuroprosthetic device’s human host.

<sup>145</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-232.

<sup>146</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-232.

<sup>147</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-232.

<sup>148</sup> See Chapter Three of this text for a discussion of neuroprosthetic devices for which 100% availability is required and any downtime presents a major hazard.

<sup>149</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-232.

the given circumstances. This could potentially prevent a motor neuroprosthetic device from being hijacked by an adversary and used to perform an action that might disclose sensitive information, cause physical or psychological harm, embarrassment, or other negative impacts for the device's human host, operator, or others.<sup>150</sup> At the same time, care must be taken that such filters do not prevent a device's host or operator from expressing legally and ethically permissible motor actions that are fully intended by the host or operator simply because they are unusual and determined by the automated filter to be anomalous or suspicious.

### Memory protection<sup>151</sup>

Traditionally, memory protection involves hardware- or software-enforced practices such as ensuring that adversaries are not able to execute code in non-executable areas of memory.<sup>152</sup>

In the case of advanced neuroprosthetic devices, it is not only the executable memory of the device's electronic components that must be protected, but also the sensory, short-term, and long-term memory of the device's human host and any memory systems that may be created jointly by the device and host acting within the device-host system.<sup>153</sup> For example, cyberattacks that are able to manipulate or otherwise affect sensory memory could potentially cause the host to perform (or not perform) physical actions in a particular manner desired by an adversary, through distorting the host's understanding of his or her environment, bodily position, or other phenomena. Manipulated or fabricated information contained within sensory memory would then compromise the host's short- and long-term memory after being transmitted to those systems. Directly manipulating the host's long-term memory could also cause a host to execute or not execute actions as desired by an adversary – for example, pressing a button that the host's long-term memory tells the host will have one effect, while in fact pressing the button

---

<sup>150</sup> For the possibility of a neuroprosthetic limb being hacked by an adversary in order to manipulate its motor activity, see Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

<sup>151</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-233.

<sup>152</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-233.

<sup>153</sup> For the possibility of developing mnemoprosthetics, see Han et al., “Selective Erasure of a Fear Memory” (2009), and Ramirez et al., “Creating a False Memory in the Hippocampus” (2013). For the possibility that an adversary might use a compromised neuroprosthetic device in order to alter, disrupt, or manipulate the memories of its host, see Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

will have a completely different effect, and the host's memory of the button's significance has been altered.

Note that there are systems and processes found (or hypothesized) within the human brain and mind that play roles analogous to those of the executable memory found in a traditional computer and which relate to human memory but may also involve other kinds of processes – for example, the visuospatial sketchpad described in the Working Memory model<sup>154</sup> or the spotlighted “theater of consciousness” described in the Global Workspace Theory.<sup>155</sup>

### Fail-safe procedures<sup>156</sup>

The design and implementation of effective fail-safe procedures is essential for ensuring information security for advanced neuroprosthetic devices and device-host systems, especially those with critical health impacts for the devices' host. Such procedures may require, for example, that the host or operator of a neuroprosthetic device receives a clear automated alert upon the failure or impending failure of critical device components, systems, or processes, along with explicit instructions of steps that should be taken. Upon some failures within certain kinds of neuroprosthetic devices, the device's host may have only minutes or seconds in which to execute specified fail-safe procedures before the failure incapacitates the host or otherwise renders him or her unable to take additional action. Other specific fail-safe procedures may include enabling mechanisms that will allow emergency medical personnel to access the neuroprosthetic device, initiating the backup of key information maintained in volatile memory, or releasing particular biochemical agents to stimulating a specific response in the body of the device's host.<sup>157</sup>

## Media protection

### Media storage and access<sup>158</sup>

It may be impractical, unethical, and illegal for an organization – in its effort to control media access – to attempt to dictate, for example, that information system media remain within the organization's secured facility when the media are contained within neuroprosthetic devices implanted within the bodies of human hosts; it may not be possible to control the location of a

<sup>154</sup> E.g., see Baddeley, “The episodic buffer: a new component of working memory?” (2000).

<sup>155</sup> See Baars, *In the Theater of Consciousness* (1997).

<sup>156</sup> NIST SP 800-53, Rev. 4 (2013), p. F-233.

<sup>157</sup> See Chapter Three of this text for a discussion of failure modes for neuroprosthetic devices and the need to provide adequate access to emergency medical personnel when a device's host is experiencing a medical emergency.

<sup>158</sup> NIST SP 800-53, Rev. 4 (2013), p. F-119-F-121.

storage medium without controlling (whether legally or unlawfully) the location of the human being in whom it is situated. If the information contained within a neuroprosthetic device is sufficiently valuable, an organization may not be able to assume that adversaries will not threaten, physically restrain, abduct, or harm the human host in whom the information's storage medium is housed in order to gain access to it.

### **Media transport<sup>159</sup>**

It may be difficult or impossible to document or restrict the transporting of storage media if they are contained in neuroprosthetic devices implanted in human hosts whose movements cannot legally or ethically be constrained.

### **Media sanitization<sup>160</sup>**

Neuroprosthetic devices or component storage units removed from a human host may contain confidential information about the host's biological and cognitive processes and sensory experiences that must be cleared, purged, or destroyed before the device can be released for reuse or disposal. Destruction of a storage medium is not necessary as long as it is guaranteed that the information cannot be retrieved from the medium or otherwise reconstructed. In the case of storage media contained within neuroprosthetic devices implanted within a human host, it may be impractical, illegal, and unethical to attempt to erase, purge, or destroy the storage medium without (or potentially even with) the host's permission.

### **Media use<sup>161</sup>**

For computers that are permanently physically located within a secured and supervised facility belonging to an organization, it may be possible for the organization to create and enforce administrative, logical, and physical controls (such as metal cages surrounding the computers<sup>162</sup>) that block users from utilizing ports or slots on the computers to insert portable storage media such as flash memory cards. In the case of neuroprosthetic devices implanted in human beings who are free to travel wherever they want and who may enter diverse kinds of environments and situations, it may not be possible to implement controls that will always reliably prevent portable storage media from being inserted into a neuroprosthetic device's slots and ports; if

---

<sup>159</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-121.

<sup>160</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-122-F-123.

<sup>161</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-124.

<sup>162</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-124.

preventing the unauthorized use of portable storage media is a priority, it may be necessary for the device's designer and manufacturer to construct the device in such a way that no such ports or connections are present and any effort to add them by an unauthorized user would destroy the device.<sup>163</sup>

## Incident response

### Incident response training<sup>164</sup>

Incident response training is especially important for the human host of an advanced neuroprosthetic device, insofar as an incident relating to such a device does not compromise or damage some external system like a desktop computer or smartphone but may actually compromise the host's own biological and cognitive processes. Once an incident is underway, a device's host may only have a very limited time in which to react and carry out response measures before losing consciousness or losing control over his or her own volition, memory, or other mental processes. Specialized incident response training can help ensure that a device's host recognizes and responds to an ongoing incident in a timely and effective manner.

### SIMULATED EVENTS<sup>165</sup>

Incidents may be especially easy to simulate for the host of a neuroprosthetic device when the device already creates a virtual or augmented reality for the host by supplying artificial sense data. At the same time, though, it may potentially be difficult for the hosts of such devices to distinguish simulated events from actual ones.<sup>166</sup>

### AUTOMATED TRAINING ENVIRONMENTS<sup>167</sup>

An organization or individual may utilize "automated mechanisms to provide a more thorough and realistic incident response training environment."<sup>168</sup> With some kinds of neuroprosthetic devices, automated training environments that are governed by artificially intelligent systems may be needed to accurately simulate or replicate the activity of adversaries whose

---

<sup>163</sup> See the device ontology in Chapter Four of this text for different aspects of a neuroprosthetic device's physical structure and accessibility, including the presence or absence of physical input and output mechanisms.

<sup>164</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-103.

<sup>165</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-104.

<sup>166</sup> See Chapter Five of this text for a discussion of the distinguishability of neuroprosthetically supplied information as an information security goal and attribute for neuroprosthetic devices.

<sup>167</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-104.

<sup>168</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-104.



capacities and techniques exceed the limits of what can be possessed and performed by an unaugmented human adversary.

## Incident response testing

### **AUTOMATED TESTING**<sup>169</sup>

Automated testing may be necessary for neuroprosthetic devices that cannot directly be accessed by technologies or activities directly controlled by human agents but which may, for example, be accessible and potentially vulnerable to attacks utilizing nanorobot swarms or other automated systems.

## Incident handling

### **AUTOMATED INCIDENT HANDLING PROCESSES**<sup>170</sup>

Relying on automated incident handling processes to perform functions of incident detection, containment, and eradication may be hazardous if the execution of such functions is able or likely to directly or indirectly cause physical or psychological harm to a neuroprosthetic device's human host; an automated incident-response system may not always recognize the effect that its efforts are inadvertently having on the device's host. On the other hand, in other situations relying on an automated incident-response system may be less likely to result in harm to a device's host than having human agents directly control the response, if the system can be trained to respond with a greater degree of speed, accuracy, and effectiveness than a human agent.

### **DYNAMIC RECONFIGURATION**<sup>171</sup>

Neuroprosthetic systems may be designed to dynamically reconfigure themselves either as a routine matter (in order to prevent potential attacks) or in response to an ongoing incident, in order "to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises."<sup>172</sup> In the case of neuroprosthetic devices utilizing biological components or physical neural networks, some degree of "dynamic reconfiguration" may be continuously taking place.<sup>173</sup>

---

<sup>169</sup> NIST SP 800-53, Rev. 4 (2013), p. F-104.

<sup>170</sup> NIST SP 800-53, Rev. 4 (2013), p. F-105.

<sup>171</sup> NIST SP 800-53, Rev. 4 (2013), p. F-105.

<sup>172</sup> NIST SP 800-53, Rev. 4 (2013), p. F-105.

<sup>173</sup> For example, for a discussion of the ways in which long-term memories stored within the human brain can undergo changes in their nature and storage over time, see Dudai, "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" (2004). In a sense, memories stored within the brain's natural neural networks that undergo such changes (even if subtle ones) over

**SUPPLY CHAIN COORDINATION<sup>174</sup>**

In some cases, successfully responding to an incident impacting an advanced neuroprosthetic device may require coordination between the device's designer, manufacturer, OS and application developers, provider, installer, operator, and human host.

**Incident monitoring<sup>175</sup>**

Conducting incident monitoring to track and document security incidents may be difficult in the case of neuroprosthetic devices (such as those comprising biological components or nanorobot swarms) that may lack a centralized mechanism capable of detecting and recording incidents affecting the device's components.<sup>176</sup>

**Incident reporting<sup>177</sup>**

Various incident-reporting complications can arise with advanced neuroprosthetic systems. For example, in the case of a human host who does not even realize that he or she has been implanted with a device, the host might realize that he or she is undergoing some unusual experience but would not associate it with the device and may have no ability to report the incident to the device's operator.<sup>178</sup>

**Incident response assistance<sup>179</sup>**

The use of dedicated organizational incident-response teams or services that proactively respond to an ongoing incident (e.g., by physically locating the host of a neuroprosthetic device, assessing his or her condition, and providing containment and recovery services) may be especially necessary in the case of neuroprosthetics whose anomalous functioning may render their host incapacitated and unable to respond to an incident himself or herself.

---

time might be thought of as loosely analogous to metamorphic or polymorphic malware: a stored memory's ongoing dynamic reconfiguration may make it more difficult for adversaries to target that particular memory for alteration, manipulation, or deletion, if the storage location and identifying characteristics of the memory are not wholly stable. See, however, the periodic discussion of the Holonomic Brain Theory throughout this text for factors that may either enhance or limit the dynamic reconfiguration of memories stored within the human brain.

<sup>174</sup> NIST SP 800-53, Rev. 4 (2013), p. F-106.

<sup>175</sup> NIST SP 800-53, Rev. 4 (2013), p. F-107.

<sup>176</sup> See the discussion of passive neuroprosthetic devices in Chapter One of this text for examples of such devices.

<sup>177</sup> NIST SP 800-53, Rev. 4 (2013), p. F-107.

<sup>178</sup> For the possibility that human hosts might unwittingly have been implanted, e.g., with certain kinds of RFID devices, see Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

<sup>179</sup> NIST SP 800-53, Rev. 4 (2013), p. F-108.

### Information spillage response<sup>180</sup>

Care must be exercised in defining information spillage with regard to advanced neuroprosthetic systems and formulating spillage responses. For example, imagine that a human host possesses a neuroprosthetic device that stores information on flash memory that the host can access and “play back” to his or her conscious awareness through sensory systems.<sup>181</sup> The host may have access and authorization to view classified information stored on the device, but viewing the information would create a (perhaps not entirely accurate) additional copy of the information in the natural long-term memory system within the host’s brain. That could potentially be considered an information spillage. A similar situation would occur if a person were authorized to read printouts of classified information while in a secured location but not to transfer the information to a digital system; if the person’s long-term memory processes were augmented with engram-storing mnemoprosthetics, simply reading the documents in an authorized manner could result in the production of an unauthorized copy of the information within the neuroprosthetic system. In such situations, manual or automated responses that seek to take “corrective action” to contain and eradicate spillage within the systems that have been “contaminated”<sup>182</sup> by the information spillage have the potential to cause physical and psychological damage to a device’s human host.

### Integrated information security analysis team<sup>183</sup>

In the case of advanced neuroprosthetic devices, an integrated information security analysis team may need to incorporate not only typical members such as “forensic/malicious code analysts, tool developers, and real-time operations personnel”<sup>184</sup> but potentially also biomedical engineers, biologists, neuroscientists, psychologists, biocyberneticists and neurocyberneticists, and implantation surgeons.<sup>185</sup>

---

<sup>180</sup> NIST SP 800-53, Rev. 4 (2013), p. F-109.

<sup>181</sup> For the idea of such sensory playback capabilities, see Merkel et al., “Central Neural Prostheses” (2007); Robinett, “The consequences of fully understanding the brain” (2002); and McGee, “Bioelectronics and Implanted Devices” (2008), p. 217.

<sup>182</sup> NIST SP 800-53, Rev. 4 (2013), p. F-109-F-110.

<sup>183</sup> NIST SP 800-53, Rev. 4 (2013), p. F-110-F-111.

<sup>184</sup> NIST SP 800-53, Rev. 4 (2013), p. F-110.

<sup>185</sup> See Chapter Three of this text for a discussion of the growing interconnection of information security with fields such as neuroscience and biomedical engineering, especially in the context of advanced neuroprosthetic devices.

## Awareness and training

### Security awareness training<sup>186</sup>

Security awareness training is important not only for the hosts or operators of neuroprosthetic devices but also for all individuals who live, work, or otherwise spend time in environments in which it is possible that other persons may possess neuroprosthetic systems that would allow them to compromise the individuals' information security.

### INSIDER THREAT<sup>187</sup>

In the case of neuroprosthetic devices that allow direct access to the cognitive processes (including sensory perceptions, thoughts, or memories) of the device's human host, complex legal and ethical questions arise over the propriety of the accessing of such information on the part of an organization's personnel in order to assess whether the human host may constitute an insider threat to the organization's information security.<sup>188</sup>

---

<sup>186</sup> NIST SP 800-53, Rev. 4 (2013), p. F-37.

<sup>187</sup> NIST SP 800-53, Rev. 4 (2013), p. F-38. For more on insider threats, see McCormick, "Data Theft: A Prototypical Insider Threat" (2008).

<sup>188</sup> See Chapter Two of this text for a discussion of other insiders within an organization who might pose a threat to a neuroprosthetic device's host or operator.



## Chapter Nine

# Technical Controls for Advanced Neuroprosthetics

In this chapter we conclude our exploration of how security controls relate to advanced neuroprosthetic devices and systems by considering in detail the families of security controls listed in *NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*, produced by the National Institute of Standards & Technology in 2013. As in the previous two chapters, we explain how particular controls that were designed for use with general-purpose computing and information systems may either: 1) become *more critical* for ensuring information security when the information system to which the control is being applied is an advanced neuroprosthetic device; 2) become *less important* or potentially even inapplicable and irrelevant within the context of an advanced neuroprosthetic device; or 3) may take on a *new and radically* different form when applied to an advanced neuroprosthetic device. In this chapter we focus on technical controls for advanced neuroprosthetics.

According to the scheme presented in *NIST SP 800-53, Rev. 4, Appendix F*, and later summarized in *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers*, technical controls include **identification and authentication, access control, audit and accountability, and system and communications protection**.<sup>1</sup>

Practices that allow for auditing and accountability (such as regular diagnostic monitoring of a neuroprosthetic device's performance and usage and the creation and analysis of logfiles) are especially important in the case of neuroprosthetic devices that have the potential to affect a user's sensory experiences or memories. Especially in cases where the user suspects the possibility of neurohacking or other manipulation, he or she may be unable or un-

---

<sup>1</sup> *NIST SP 800-100* (2006), p. iii.

willing to trust the contents of his or her own memory and sensory experiences.<sup>2</sup> In such circumstances, logfiles can provide an objective external reference point that allows the user to reconstruct the origin and nature of the device's activity and develop an account of the truth or falsity of his or her experiences – assuming that the user can have confidence in the methods used to maintain and access the logfiles and that the user's experience of the logfiles might not itself be an illusion or fabrication.<sup>3</sup>

Note that in the model presented in *NIST SP 800-53*, identification and authentication are not considered to be elements of access control; instead both identification and authentication and the separate process of access control are envisioned as different forms of technical controls. Other models arrange these elements differently – for example, Rao and Nayak make identification, authentication, and authorization different aspects of access controls, which are manifested in the three “layers” of administrative, technical, and physical controls.<sup>4</sup> Thus depending on the framework, access controls can be considered a kind of technical control, or *vice versa*.

In this chapter we consider in more detail the idea of an “access control” as understood to include both authentication and authorization as constituent components. When referring to the range of access controls referred to by Rao and Nayak as “technical controls,” we will refer to it by its alternative name of “logical controls,” to distinguish it from “technical controls” as used in the sense of *NIST SP 800-53*.

## Identification and authentication

### Identification and authentication (organizational users)<sup>5</sup>

---

<sup>2</sup> For a discussion of attacks that may be intended to induce long-term changes in the neural activity or structures of a neuroprosthetic device's human host, see Denning et al., “Neurosecurity: Security and Privacy for Neural Devices” (2009).

<sup>3</sup> For the possibility that a device designed to receive raw data from the external environment could have that data replaced with alternative data transmitted from some external information system, see Koops & Leenes, “Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes” (2012). Regarding the possibility of neuroprosthetics being used to provide falsified data or information to their hosts or users, see also McGee, “Bioelectronics and Implanted Devices” (2008), p. 221. See also Gladden, “Tachikomatic Domains: Utopian Cyberspace as a ‘Contingent Heaven’ for Humans, Robots, and Hybrid Intelligences” (2015).

<sup>4</sup> Rao & Nayak, *The InfoSec Handbook* (2014), pp. 62-69.

<sup>5</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-91.

For neuroprosthetic devices that are acquired and operated by individual human hosts as consumer electronics devices, the robust systems for identifying and authenticating users that are utilized within large institutions with dedicated IT and InfoSec personnel may not be available. On the other hand, for some kinds of neuroprosthetic devices, a device may only physically be capable of interacting with the single human being in whose body the device is initially installed, thus eliminating both the need and ability to create multiple user accounts or distinguish between organizational and non-organizational users.

### **SINGLE SIGN-ON<sup>6</sup>**

If a single human host has multiple neuroprosthetic devices installed, it may be desirable for a single system (e.g., one that has direct access to the user's cognitive activity and which can be controlled by the user's thoughts) to serve as the user's interface with the collection of devices; logging on to that single gateway device simultaneously gives the user access to the other implanted systems.

## **Device identification and authentication**

### **DEVICE ATTESTATION<sup>7</sup>**

Device attestation performs “the identification and authentication of a device based on its configuration and known operating state.”<sup>8</sup> Some neuroprosthetic devices (such as those consisting of physical neural networks<sup>9</sup> or biological components<sup>10</sup>) may not possess stable, clearly definable configurations or operating states that can be used as the basis for device attestation. However, it may be possible to perform attestation on the basis of a cryptographic hash<sup>11</sup> that is stored within the device or its components, even if that information is not directly utilized by the device itself in performing its normal functions.

---

<sup>6</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-92.

<sup>7</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-94.

<sup>8</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-94.

<sup>9</sup> See the device ontology in Chapter Four of this text for a discussion of such devices.

<sup>10</sup> For the possibility of neuroprosthetic devices involving biological components, see Merkel et al., “Central Neural Prostheses” (2007). For discussion of a hybrid biological-electronic interface device (or “cultured probe”) that includes a network of cultured neurons on a planar substrate, see Rutten et al., “Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe” (2007). Hybrid biological-electronic interface devices are also discussed by Stieglitz in “Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems” (2007).

<sup>11</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-94.



## Identifier management<sup>12</sup>

For neuroprosthetic devices that automatically run once activated, without requiring a system logon – or which simply verify that they possess an active physical and biological interface with a human host, without determining who that host is<sup>13</sup> – the device may not utilize any user or administrator accounts and thus there will not be unique account identifiers.

In other cases, the identifier for the device's human host (or operator) may not be an account name or string of text as commonly used but may potentially be an image, sound, electromechanical stimulus, or some other kind of information that in other kinds of systems may typically be used for purposes of authentication rather than identification.

## Authenticator management

### PASSWORD-BASED AUTHENTICATION<sup>14</sup>

For some kinds of neuroprosthetic devices that interface directly with the conscious mental processes of their human host, the host's authenticator could potentially be a particular thought or memory (or the context surrounding the memory) rather than a password as understood in the traditional sense of a discrete string of characters.<sup>15</sup> An internal thought used as a password may take on a slightly different form each time it is expressed by its user, thus it may need to be authenticated using some statistical means (perhaps using a neural network) rather than determining whether it precisely matches some discrete piece of information used as a reference.

### NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS<sup>16</sup>

In the case of neuroprosthetic devices that store information in the form of a physical neural network, it may not be possible to force (or even enable) the system to store its information in a form that utilizes traditional encryption methods.

---

<sup>12</sup> NIST SP 800-53, Rev. 4 (2013), p. F-94.

<sup>13</sup> See Chapter Three of this text and its discussion of biometrics for the possibility that a neuroprosthetic device might detect whether it is situated within a living human being.

<sup>14</sup> NIST SP 800-53, Rev. 4 (2013), p. F-96-F-97.

<sup>15</sup> See Thorpe et al., "Pass-thoughts: authenticating with our minds" (2005). Mizraji et al., in "Dynamic Searching in the Brain" (2009), use the word "password" in a more metaphorical sense than the typical meaning in information security, but the dynamic memory searching mechanisms that they describe could potentially also serve as the basis for an authentication system.

<sup>16</sup> NIST SP 800-53, Rev. 4 (2013), p. F-97-F-98.

**HARDWARE TOKEN-BASED AUTHENTICATION<sup>17</sup>**

For implantable neuroprosthetic systems, it may be possible to utilize a hardware token-based authenticator that is implanted elsewhere in the body of a neuroprosthetic device's human host. While the physical proximity of the hardware token to the neuroprosthetic device does not guarantee the fact that the device is still implanted within its human host, the fact that the hardware token is no longer in physical proximity to the neuroprosthetic device may indicate either that the neuroprosthetic device has been removed from its host (and should thus automatically deactivate itself and potentially wipe stored information) or that the security of the portion of the host's body in which the token was stored has been compromised (which, in some circumstances, may also be a condition that should trigger automatic deactivation of the neuroprosthetic device and the wiping of information stored within it).

It is also possible that implanted neuroprosthetic devices themselves could be used as authenticators to grant their host access to other (external) information systems.<sup>18</sup>

**BIOMETRIC-BASED AUTHENTICATION<sup>19</sup>**

Traditional biometric methods do not provide an exact match between the biometric data presented by the individual who desires to access the system and the stored biometric data used as an authenticator; a number of both false positives and false negatives are to be expected.<sup>20</sup> Because of their unique (and potentially long-term or even permanent) interface with the biological structures and processes of their human host, neuroprosthetic devices may be able to utilize newly developed biometric technologies and methods that are not possible for other kinds of information systems.<sup>21</sup>

**Authenticator feedback<sup>22</sup>**

Insofar as the process of identification and authentication might take place entirely within the private cognitive processes of a neuroprosthetic device's human host, it may be possible for the device to provide full authentication feedback (e.g., displaying the actual characters of a password that is

---

<sup>17</sup> NIST SP 800-53, Rev. 4 (2013), p. F-98.

<sup>18</sup> For the use of RFID implants as authenticators, see Rotter et al., "Potential Application Areas for RFID Implants" (2012). See Chapter Three of this text for a discussion of the advantages and disadvantages of using external hardware tokens to allow medical personnel emergency access to an IMD.

<sup>19</sup> NIST SP 800-53, Rev. 4 (2013), p. F-98.

<sup>20</sup> NIST SP 800-53, Rev. 4 (2013), p. F-98.

<sup>21</sup> See Chapter Three of this text for a discussion of unique possibilities for the use of biometrics with neuroprosthetic devices.

<sup>22</sup> NIST SP 800-53, Rev. 4 (2013), p. F-99.

being mentally “typed” by the device’s host, without replacing the characters with asterisks to obscure their value) to the device’s host without worrying that the feedback may be observed or intercepted by unauthorized parties using methods such as shoulder surfing.

## Identification and authentication (non-organizational users)

### **ACCEPTANCE OF THIRD-PARTY CREDENTIALS<sup>23</sup>**

Allowing the use of third-party credentials to authenticate non-organizational users of a neuroprosthetic device may be one approach to addressing the fact that, for example, the human host of a neuroprosthetic device might experience a medical emergency when he or she is in a public place or otherwise unable to rely on specialized medical support services provided by members of his or her institution. In such a circumstance, emergency medical responders who have no previous association with the device’s host or operator may need to acquire immediate full access to the devices and its functionality and an ability to override existing settings and control its operation in order to offer the host medical treatment and avoid harm to himself or herself or others. It may be possible for local, national, or international governmental agencies, licensing and certification bodies, or associations of licensed medical personnel or other first responders to serve as third parties issuing credentials to individual personnel which the designers, manufacturers, and operators of advanced neuroprosthetic devices will allow devices to accept as authenticators – either universally, or perhaps only when the neuroprosthetic device detects that its user has entered a particular biological state or is experiencing a particular medical condition.<sup>24</sup>

### **Adaptive identification and authentication<sup>25</sup>**

Some neuroprosthetic devices may utilize adaptive identification and authentication. For example, the host or operator of a motor neuroprosthetic may be able to operate an artificial limb within certain nominal physical parameters without requiring special identification, but attempting to instruct

---

<sup>23</sup> NIST SP 800-53, Rev. 4 (2013), p. F-100.

<sup>24</sup> For a discussion of certificate schemes, see, Chapter Three of this text and, e.g., Cho & Lee, “Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks” (2012), and Freudenthal et al., “Practical techniques for limiting disclosure of RF-equipped medical devices” (2007). Regarding the ability of IMDs to detect a medical emergency that is being experienced by their human host, see Denning et al., “Patients, pace-makers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010), pp. 921-22.

<sup>25</sup> NIST SP 800-53, Rev. 4 (2013), p. F-102.

the limb to operate in a way that would create a danger of significant damage to the device or its host may trigger a request from the system for additional authentication information before the instruction is executed. Similarly, for reasons of physical or psychological safety, an artificial eye or ear might possess built-in artificial constraints in the kind or quantity of incoming information that will be allowed to reach the conscious awareness of its human host; disabling such filters on the brightness of visual data or loudness of auditory data might be possible only after successfully submitting additional authentication information.<sup>26</sup>

## Access control

### Account management<sup>27</sup>

Some implantable neuroprosthetic devices may not possess multiple “accounts” that allow a device’s operator or host to log into the system; the device may simply begin running once supplied with power and activated. In effect, such a device has a single account with an automatic login. Other devices may have specialized accounts for a device’s operator(s) and potentially its human host.

#### REMOVAL OF TEMPORARY/EMERGENCY ACCOUNTS<sup>28</sup>

Implementing the automatic deletion of emergency accounts after a predetermined time (rather than through manual action of the operator) may create a potential danger to the health and safety of the device’s host, if an emergency account were being used to access the device in order to perform an urgent repair or provide some emergency medical service.

#### INACTIVITY LOGOUT<sup>29</sup>

Implementing an automatic logout after a predetermined period of activity should be done only after careful consideration, given the fact that a device’s operator or host may expect and sometimes require instantaneous access to the device’s functionality, and the delay caused by a need to log into an account would be unacceptable and potentially hazardous.

---

<sup>26</sup> For a discussion of psychological, social, and cultural factors that might cause the host of an implanted device to intentionally ignore, disable, or otherwise subvert a device’s security features and mechanisms – even to the extent of causing self-harm – see Denning et al., “Patients, pace-makers, and implantable defibrillators: Human values and security for wireless implantable medical devices” (2010).

<sup>27</sup> NIST SP 800-53, Rev. 4 (2013), p. F-7.

<sup>28</sup> NIST SP 800-53, Rev. 4 (2013), p. F-9.

<sup>29</sup> NIST SP 800-53, Rev. 4 (2013), p. F-9.

**ACCOUNT MONITORING / ATYPICAL USAGE<sup>30</sup>**

For some kinds of neuroprosthetic devices, it may be difficult to establish clear baselines and a definition of what constitutes “typical” and “atypical” usage, just as it is difficult to clearly define what constitutes “typical” thoughts, emotions, beliefs, volitions, or use of the imagination. This challenge may be exacerbated when a neuroprosthetic device is used to allow a user to interface with and experience some virtual environment which is in a sense already “atypical” and likely to generate new kinds of activities and experiences.<sup>31</sup>

**DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS<sup>32</sup>**

Even if the operator or human host of a neuroprosthetic device has been clearly identified as a “high-risk individual” who is likely to use the device to cause harm or for unauthorized purposes, the decision of whether to disable the individual’s account may raise serious legal and ethical questions, if disabling the account could impair (or even wholly terminate) the functioning of the device, thereby causing physical or psychological harm to the device’s host or to others who would in some way be affected.

**Access enforcement****DUAL AUTHORIZATION<sup>33</sup>**

Controls requiring the approval of two different authorized parties before instructions will be executed may be impractical and inappropriate in the case of neuroprosthetic devices that are operated by their human host and which must be able to function when the host is operating in an open environment in which the device cannot be accessed by any other parties (e.g., a remote area without cell phone service or Internet access).

**MANDATORY ACCESS CONTROL<sup>34</sup>**

In some cases it may be inappropriate and potentially unethical and illegal to implement mandatory (non-discretionary) access controls which, for example, prevent a device’s human host from granting others access to information stored in or generated with the aid of the neuroprosthetic device. For

---

<sup>30</sup> NIST SP 800-53, Rev. 4 (2013), p. F-10.

<sup>31</sup> For some examples of neuroprosthetic devices that provide their hosts and users, e.g., with “the experience of a new body that is radically *nonhuman*,” see Gladden, “Cybershells, Shapeshifting, and Neuroprosthetics” (2015).

<sup>32</sup> NIST SP 800-53, Rev. 4 (2013), p. F-10.

<sup>33</sup> NIST SP 800-53, Rev. 4 (2013), p. F-11.

<sup>34</sup> NIST SP 800-53, Rev. 4 (2013), p. F-11.

example, imagine a neuroprosthetic device that enhances its human host's powers of imagination;<sup>35</sup> if the end user license agreement specifies that the host is the sole owner of all intellectual property (such as thoughts and ideas) that are generated with the aid of the device, the device should not include controls which attempt to place mandatory limits on the user's ability to share that property with others and which block the user from utilizing his or her discretion in extending access rights to others.

#### **CONTROLLED RELEASE<sup>36</sup>**

It may be difficult or impossible to prevent the release of information beyond the boundaries of the neuroprosthetic system if the mind of the human host is a part of that system, as the mind can express and convey information through speech, gestures, and other means.

### **Information flow enforcement**

#### **DYNAMIC INFORMATION FLOW CONTROL<sup>37</sup>**

Particular kinds of information flows could be enabled or disabled if, for example, the neuroprosthetic device detects that its human host is experiencing a medical emergency or if the device's operator determines that the host is entering a situation in which specialized information flows are warranted.

#### **EMBEDDED DATA TYPES<sup>38</sup>**

Controls may need to be implemented to ensure, for example, that sense data being received from the external environment by an artificial sensory organ does not contain embedded patterns of data that would be detected and interpreted by the device as (potentially malicious) executable code.<sup>39</sup>

---

<sup>35</sup> See Cosgrove, "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation" (2004); Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); and Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015).

<sup>36</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-13.

<sup>37</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-15.

<sup>38</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-15.

<sup>39</sup> For an example that may not literally involve the use of potentially malicious executable code – but whose method of reception by a device and effects on a device are suggestive of such possibilities – see Hansen and Hansen, who discuss the hypothetical case of a poorly designed prosthetic eye whose internal computer can be disabled if the eye is presented with a particular pattern of flashing lights. See Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

**SECURITY POLICY FILTERS<sup>40</sup>**

Security policy filters may be implemented in order to filter, for example, the kinds of auditory sense data that are permanently recorded by an artificial ear not because the device itself is technologically incapable of recording certain kinds of information but because it should not be permanently recorded due to information security considerations.

**DETECTION OF UNSANCTIONED INFORMATION<sup>41</sup>**

Controls may be used, for example, to detect proprietary information or classified information whose possession would be illegal and block it from being transferred into a host's memory by the neuroprosthetic device.

**DOMAIN AUTHENTICATION<sup>42</sup>**

Even when a neuroprosthetic device is intended solely to transmit information between different systems that are permanently embedded within the body of its human host and not to the external environment, controls may need to be implemented to ensure that the "source and destination points" of information are indeed the intended systems.<sup>43</sup>

**PHYSICAL/LOGICAL SEPARATION OF INFORMATION FLOWS<sup>44</sup>**

For some kinds of neuroprosthetic devices (e.g., those utilizing physical neural networks) it may be extremely difficult to segregate different kinds of information moving through the system.<sup>45</sup>

**Separation of duties<sup>46</sup>**

Separation of duties may be difficult to implement in cases in which a single person is both the operator and human host of a neuroprosthetic device, as well as potentially the developer of applications or other content for use by the device. (Indeed, for some kinds of passive neuroprosthetics, the brain

---

<sup>40</sup> NIST SP 800-53, Rev. 4 (2013), p. F-16.

<sup>41</sup> NIST SP 800-53, Rev. 4 (2013), p. F-17.

<sup>42</sup> NIST SP 800-53, Rev. 4 (2013), p. F-17.

<sup>43</sup> NIST SP 800-53, Rev. 4 (2013), p. F-17.

<sup>44</sup> NIST SP 800-53, Rev. 4 (2013), p. F-18.

<sup>45</sup> For example, if various holographic or holonomic models of the human brain's cognitive processing and memory storage are correct, it may be difficult or impossible to isolate a certain small group of neurons as "containing" a particular memory or thought. For discussion of such issues, see, e.g., Longuet-Higgins, "Holographic Model of Temporal Recall" (1968); Pribram, "Prolegomenon for a Holonomic Brain Theory" (1990); and Pribram & Meade, "Conscious Awareness: Processing in the Synaptodendritic Web..." (1999).

<sup>46</sup> NIST SP 800-53, Rev. 4 (2013), p. F-18.

of the human host may also be providing the “operating system” for the device.<sup>47</sup>)

## Least privilege

### **NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS<sup>48</sup>**

With some kinds of neuroprosthetic devices, it may be a technological and functional necessity for a device’s operator or host to possess privileged access to the system, even when it is being used to perform non-security functions.

### **PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS<sup>49</sup>**

Fully blocking non-organizational users from exercising privileged access to a neuroprosthetic system may not be possible if the system must possess mechanisms allowing privileged access (e.g., by medical personnel) in the case of a medical emergency affecting the device’s human host.<sup>50</sup>

## Unsuccessful logon attempts<sup>51</sup>

A control that automatically locks an account or delays the next logon prompt after a specified number of consecutive unsuccessful logon attempts may be hazardous in emergency situations in which access to the device is needed immediately in order to prevent physical or psychological harm to the human host or others (and which may be precisely the sort of situation in which ongoing stress or physical impairment may cause the host’s logon attempts to be unsuccessful).<sup>52</sup>

### **PURGE/WIPE MOBILE DEVICE<sup>53</sup>**

A control that automatically purges data from a neuroprosthetic device after a certain number or type of unsuccessful logon attempts may be desirable in order to preserve the confidentiality and possession of sensitive data stored within the device. On the other hand, such countermeasures may be legally or ethically impermissible in situations in which they would cause physical or psychological damage to a device’s host or to others.

<sup>47</sup> See Chapter One of this text for a discussion of passive neuroprosthetic devices.

<sup>48</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-19.

<sup>49</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-20.

<sup>50</sup> See Chapter Three of this text for an in-depth discussion of issues relating to emergency access to neuroprosthetic devices for medical personnel.

<sup>51</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-21.

<sup>52</sup> See Chapter Three of this text for alternative methods for preventing resource depletion attacks that involve a string of unsuccessful logon attempts, and see Chapter Two for a basic description of resource depletion attacks.

<sup>53</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-21.



### Concurrent session control<sup>54</sup>

For some kinds of neuroprosthetic devices (e.g., those that include a physical neural network that interacts directly with the memory mechanisms of their host's brain), the number of concurrent sessions may be limited for technological reasons to a single session – namely, that of the device's human host.

### Session lock<sup>55</sup>

Automatically terminating a session after a predetermined period of inactivity may be hazardous with neuroprosthetic devices whose operator and host expect or require that the device always be ready to provide access and service, without the delay that would be required for reauthentication.<sup>56</sup>

### Session termination<sup>57</sup>

Session termination may be impossible to implement for some kinds of neuroprosthetic devices. A device consisting of synthetic neurons that are fully integrated into the neural network of their host's brain may in effect run a single “session” that will last throughout the host's remaining lifetime.

### Permitted actions without identification or authentication<sup>58</sup>

Some advanced neuroprosthetic systems (e.g., those based on a physical platform utilizing nanorobots or synthetic neurons) may not be capable of carrying out user identification or authentication; in these cases, the devices may permit and perform all possible actions without identification or authentication.

### Remote access<sup>59</sup>

A neuroprosthetic device implanted in a human host may need to remotely access systems that belong, e.g., to the device's manufacturer, operator, or a dedicated medical support team. Automated monitoring, encryption,

---

<sup>54</sup> NIST SP 800-53, Rev. 4 (2013), p. F-23.

<sup>55</sup> NIST SP 800-53, Rev. 4 (2013), p. F-23.

<sup>56</sup> See Chapter Three of this text for a discussion of the need for 100% availability for some kinds of neuroprosthetic devices.

<sup>57</sup> NIST SP 800-53, Rev. 4 (2013), p. F-24.

<sup>58</sup> NIST SP 800-53, Rev. 4 (2013), p. F-24-F-25.

<sup>59</sup> NIST SP 800-53, Rev. 4 (2013), p. F-28.

and the use of managed access control points may be desirable in such circumstances. Such access need not necessarily be wireless, if a neuroprosthetic device has an external port that allows for a wired connection.

## Wireless access

### TRANSMISSION POWER LEVELS<sup>60</sup>

Limiting the power levels of wireless transmissions from a mobile device or utilizing directional antennas is a useful practice for reasons of ensuring information security; in the case of some implantable neuroprosthetic devices it may also be desirable to help ensure the long-term health and safety of the device's host and avoid undesirable interference with other implanted systems.<sup>61</sup>

## Access control for mobile devices

### FULL DEVICE / CONTAINER-BASED ENCRYPTION<sup>62</sup>

Although desirable from an information security perspective, full-device encryption and container-based encryption may not be possible for the contents of some kinds of neuroprosthetic devices, such as those storing information in a physical neural network.

## Use of external information systems<sup>63</sup>

Insofar as the information within a neuroprosthetic system can be accessed by the mind of its host, it is possible (and in some situations perhaps likely) that the information will eventually be transmitted to or copied – in a manner that may or may not accurately reflect the original source information – into external information systems to which the host's mind has access (e.g., the host's personal computer, smartphone, or other systems).

### PORTABLE STORAGE DEVICES<sup>64</sup>

Some neuroprosthetic devices that possess an external port, media slot, or socket may allow information to be easily copied to or from portable storage media or devices, with significant implications for information security.<sup>65</sup>

---

<sup>60</sup> NIST SP 800-53, Rev. 4 (2013), p. F-30.

<sup>61</sup> See Chapter Three of this text for a discussion of the reliance on wireless communication with external systems that is characteristic of many kinds of implantable neuroprosthetic devices.

<sup>62</sup> NIST SP 800-53, Rev. 4 (2013), p. F-31.

<sup>63</sup> NIST SP 800-53, Rev. 4 (2013), p. F-32.

<sup>64</sup> NIST SP 800-53, Rev. 4 (2013), p. F-33.

<sup>65</sup> See the device ontology in Chapter Four of this text for a discussion of such input and output mechanisms for neuroprosthetic devices.

**NON-ORGANIZATIONALLY OWNED SYSTEMS/COMPONENTS/DEVICES<sup>66</sup>**

Neuroprosthetic devices may operate within a complex context in which, for example, key components of a device are owned by an organization but other components consist of biological matter that is a part of the host's body. This may complicate the process of establishing controls for the sharing of information with components or systems that are not owned by the organization.

**Data mining protection<sup>67</sup>**

Some kinds of neuroprosthetic devices (such as those that utilize physical neural networks and holonomic storage mechanisms) may inherently possess robust protections against many typical data-mining technologies or techniques.

**Audit and accountability<sup>68</sup>****Audit events<sup>69</sup>**

In the case of some neuroprosthetic devices (such as those that utilize a physical neural network or are passive devices controlled by the host's neural circuitry<sup>70</sup>) it may be difficult to specify particular kinds of auditable events.

**Audit storage capacity<sup>71</sup>**

Implantable neuroprosthetic devices may possess limited onboard capacity to store audit records generated by the device. Offloading audit data to external systems for permanent storage may not be possible, for example, if a neuroprosthetic device includes a physical neural network with billions of neurons whose individual real-time actions have been designated as audit events but which cannot be recorded and transmitted to external systems using current or foreseeable technologies.

---

<sup>66</sup> NIST SP 800-53, Rev. 4 (2013), p. F-33.

<sup>67</sup> NIST SP 800-53, Rev. 4 (2013), p. F-35.

<sup>68</sup> For the importance of auditing for IMDs, see Hansen & Hansen, "A Taxonomy of Vulnerabilities in Implantable Medical Devices" (2010).

<sup>69</sup> NIST SP 800-53, Rev. 4 (2013), p. F-41-F-42.

<sup>70</sup> See the device ontology in Chapter Four of this text for a discussion of neuroprosthetic devices that utilize a physical neural network and Chapter One for a discussion of passive neuroprosthetic devices.

<sup>71</sup> NIST SP 800-53, Rev. 4 (2013), p. F-43.

## Response to audit processing failures

### SHUTDOWN ON FAILURE<sup>72</sup>

For some kinds of advanced neuroprosthetic devices it may be essential that the device automatically shut down if its audit-processing ability is compromised (e.g., due to a hardware error or reaching the audit storage capacity), in order to avoid the possibility that the loss of audit-processing ability might allow the device to inflict physical or psychological harm on its host or others. In other cases, a device may be required to continue operating after audit-processing ability has been compromised and until it can be restored, due to the fact that in the absence of an audit-processing ability, the cessation of operations could inflict harm.

### Protection of audit information<sup>73</sup>

The use of hardware-enforced write-once media, cryptographic protection, read-only access, and backup on separate physical systems is beneficial for ensuring information security for a neuroprosthetic device's audit information.<sup>74</sup> However, the use of such technologies and techniques may or may not be possible for a neuroprosthetic device. For example, an implanted device may have no means of backing up audit data to external systems.<sup>75</sup>

## Non-repudiation

### CHAIN OF CUSTODY<sup>76</sup>

The chain of custody of audit information may be difficult or impossible to maintain for a neuroprosthetic device that stores audit information within itself (without the possibility of backup to external systems) and which is not stored permanently within a single secured facility belonging to the operator but is implanted in a human being who brings the device into environments and situations in which unauthorized attempts to access the device may be made.

## Session audit<sup>77</sup>

---

<sup>72</sup> NIST SP 800-53, Rev. 4 (2013), p. F-44.

<sup>73</sup> NIST SP 800-53, Rev. 4 (2013), p. F-49.

<sup>74</sup> NIST SP 800-53, Rev. 4 (2013), p. F-49.

<sup>75</sup> See Chapter Five of this text for the distinction between information stored by neuroprosthetic devices in the form of engrams vs. exograms; information stored using exograms is typically easier to backup to external systems.

<sup>76</sup> NIST SP 800-53, Rev. 4 (2013), p. F-50.

<sup>77</sup> NIST SP 800-53, Rev. 4 (2013), p. F-53.

Monitoring the ways in which the operator or host utilizes a neuroprosthetic device raises legal and ethical questions insofar as such monitoring may capture and record personal medical data, the contents of cognitive processes, or other sensitive data about the status and actions of the device's human host.<sup>78</sup>

## System and communications protection

### Application partitioning<sup>79</sup>

Separating a system's user functionality and interface services from its administrative and system management functionality<sup>80</sup> may be difficult or impossible in the case of a neuroprosthetic device whose human host is also its operator. In other cases, such partitioning may be not only desirable but necessary, for example if a device's host is the "user" responsible for controlling some aspects of a device's ongoing operation but management of key medical and technical aspects of the device's behavior is controlled by remote "users" in the form of a team of specialized medical and IT personnel who possess expert knowledge that the human host lacks.<sup>81</sup>

### Security function isolation

#### **HARDWARE SEPARATION<sup>82</sup>**

Hardware separation mechanisms may be utilized, for example, to segregate the systems of a neuroprosthetic device that interact directly with the neural circuitry of the device's host from those which relate to the device's power supply or wireless communication with external systems.

#### **ACCESS/FLOW CONTROL FUNCTIONS<sup>83</sup>**

Security functions that can (and ideally should) be segregated from the access and flow-control enforcement functions built into a device include

---

<sup>78</sup> Regarding such legal and ethical issues, see, e.g., Hildebrandt & Anrig, "Ethical Implications of ICT Implants" (2012); Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012); McGrath & Scanaill, "Regulations and Standards: Considerations for Sensor Technologies" (2013); and Shoniregun et al., "Introduction to E-Healthcare Information Security" (2010).

<sup>79</sup> NIST SP 800-53, Rev. 4 (2013), p. F-184.

<sup>80</sup> NIST SP 800-53, Rev. 4 (2013), p. F-184.

<sup>81</sup> See Chapter Three of this text for a discussion of the distinction between a neuroprosthetic device's human host and its user or users.

<sup>82</sup> NIST SP 800-53, Rev. 4 (2013), p. F-185.

<sup>83</sup> NIST SP 800-53, Rev. 4 (2013), p. F-185.

“auditing, intrusion detection, and anti-virus functions.”<sup>84</sup> In the case of some neuroprosthetic devices (e.g., those utilizing a physical neural network) it may not be possible to isolate such functions if they are both stored and executed holonomically by components which execute many (or all) of a device’s functions.<sup>85</sup>

#### MODULE COUPLING AND COHESIVENESS<sup>86</sup>

It is a best practice to develop and utilize “security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.”<sup>87</sup> In the case of highly sophisticated multimodal neuroprosthetic devices, it may be possible to develop separate security functions that separately address, for example, security relating to incoming sense data (with data from each sensory organ handled separately), internal cognitive activities (with each activity possessing its own security functions), and outgoing motor instructions (with different security functions for each motor modality and plant. The development of independent modules may not be possible with other kinds of neuroprosthetic devices (e.g., those that utilize a physical neural network or which store and process information holographically).

#### Information in shared resources<sup>88</sup>

Care must be given to ensuring information security in situations in which other users, accounts, or processes may have access to shared system resources through which information created or used by or otherwise related to a neuroprosthetic device has passed or within which it has been stored. In such circumstances information security is pursued through the control of **object reuse** and **residual information protection**.<sup>89</sup> Similar but distinct concerns include the need to address situations of **information remanence** in which action has been undertaken to erase or destroy information (and it may nominally be designated by the system as “deleted”) but residual traces of the data still exist and can potentially be accessed,<sup>90</sup> as well as situations in which

<sup>84</sup> NIST SP 800-53, Rev. 4 (2013), p. F-185.

<sup>85</sup> See Longuet-Higgins, “Holographic Model of Temporal Recall” (1968); Pribram, “Prolegomenon for a Holonomic Brain Theory” (1990); and Pribram & Meade, “Conscious Awareness: Processing in the Synaptodendritic Web...” (1999).

<sup>86</sup> NIST SP 800-53, Rev. 4 (2013), p. F-186.

<sup>87</sup> NIST SP 800-53, Rev. 4 (2013), p. F-186.

<sup>88</sup> NIST SP 800-53, Rev. 4 (2013), p. F-186.

<sup>89</sup> NIST SP 800-53, Rev. 4 (2013), p. F-186.

<sup>90</sup> With regard to the case of information stored within a physical neural network – and perhaps even within the human brain’s natural long-term memory storage systems – researchers have had some success with attempting to manipulate or delete specific memories stored within the brains of mice; see Han et al., “Selective Erasure of a Fear Memory” (2009). However, it is unclear

**covert channels** are utilized to access, transmit, or manipulate information in ways that bypass information flow restrictions, potentially by employing a device's systems, components, or processes in imaginative or counterintuitive ways that were never anticipated by the device's designer.<sup>91</sup>

For some neuroprosthetic devices, "shared resources" may include biological systems of a device's human host (such as the circulatory system, sensory organs, or limbs) or the host's cognitive systems and processes (such as natural memory storage systems and particular mnemonic content or memories); the use of a neuroprosthetic device may create traces of information in such shared systems that can be accessed by other processes or users of the device or other implanted devices within the host's body, even if they lack direct access to the account, components, and processes within the neuroprosthetic device that created the original information.

### Denial of service protection<sup>92</sup>

Denial of service attacks may take on new forms in the cases of some advanced neuroprosthetic devices. For example, a sensory neuroprosthetic such as an artificial eye could potentially be subject to a successful denial of service attack by exposing it to an intense light source or array of light sources that overwhelms, confuses, or blocks its ability to gather desired information from the environment. Denial of service attacks can also take the form of **resource depletion attacks** that attempt to exhaust the internal battery or other power source of an implantable neuroprosthetic device by subjecting it to an unending string of wireless access requests from some external system: even if the neuroprosthetic device successfully rejects all of the unauthorized access requests, the work of responding to and verifying each request can quickly exhaust the device's battery and disable it.<sup>93</sup>

### Resource availability<sup>94</sup>

---

to what extent, if any, it might someday be possible to "delete" or "erase" intricate long-term memories stored within the natural long-term memory systems of human brains; information remanence may thus become a complex and major challenge for neuroprosthetic devices utilizing physical neural networks, biological components, and engrams for the storage of information. Such issues surrounding the possibility of deleting long-term memories may become even more vexing if, e.g., holographic or holonomic models of the brain's memory systems are correct.

<sup>91</sup> NIST SP 800-53, Rev. 4 (2013), p. F-186.

<sup>92</sup> NIST SP 800-53, Rev. 4 (2013), p. F-187.

<sup>93</sup> See the discussion of threats in Chapter Two of this text for more about resource depletion attacks.

<sup>94</sup> NIST SP 800-53, Rev. 4 (2013), p. F-187.

Priority protection<sup>95</sup> may be utilized, for example, to ensure that a neuroprosthetic device's processes that control and enable the proper functioning of the respiratory and circulatory systems of their human host's body enjoy higher-priority access to the device's resources than processes that provide an augmented-reality enhancement to the user's vision which is useful but not critically necessary. Quotas<sup>96</sup> may be utilized to ensure that a particular process does not consume excessive resources, even when there is no other immediate demand for the resources; the use of such quotas can help ensure that spare resources are available for instantaneous access should they be required by another process (particularly a high-priority one) which needs the resources immediately in order to execute some critical task or prevent harm to the device's host or user.

### Boundary protection<sup>97</sup>

Boundary protection is of critical importance for advanced neuroprosthetic devices and takes on new meanings in this context. An information system should monitor (and, as appropriate, control) all communications taking place at the system's external boundary which cause data or information to enter or leave the system as well as communications taking place across key internal boundaries within the device.<sup>98</sup> In the case of advanced neuroprosthetic devices, key boundaries include the:

- Physical boundary between the neuroprosthetic device and the biological matter of the device's human host. (And in particular, the physical boundary or interface between the device and natural neurons within the host's body.)<sup>99</sup>
- Physical boundary between the neuroprosthetic device and the environment external to the host's body (for prostheses that are exposed to the external environment). This may include a boundary with particular systems, devices, or individuals located within that external environment.
- Physical boundary between the host's body and the surrounding external environment.<sup>100</sup>

<sup>95</sup> NIST SP 800-53, Rev. 4 (2013), p. F-187.

<sup>96</sup> NIST SP 800-53, Rev. 4 (2013), p. F-187.

<sup>97</sup> NIST SP 800-53, Rev. 4 (2013), p. F-188.

<sup>98</sup> NIST SP 800-53, Rev. 4 (2013), p. F-188.

<sup>99</sup> See Chapter One of this text and the device ontology in Chapter Four for a discussion of different kinds of neural interfaces.

<sup>100</sup> For a discussion of the significance of the physical boundaries of a human organism and the ways in which technologies such as implantable neuroprosthetics can impact cognitive processes and the "moral sense of person" vs. "the notion of person as a subject of experiences," see Buller, "Neurotechnology, Invasiveness and the Extended Mind" (2011).



- Physical boundary between the neuroprosthetic device and other implanted devices within the host's body.
- Physical, physiological, psychological, and logical boundaries between different neuronal processes within the device-host system – such as the boundary at which environmental stimuli are transduced into electrochemical signals by sensory organs and the boundary at which raw sense data is transformed into sensory perceptions within the host's mind. Also included are psychological boundaries between phenomena such as memory, emotion, volition, and conscience whose phenomenological<sup>101</sup> and experiential boundaries from the perspective of the mind of a device's human host may not clearly correspond to physical boundaries within the device-host system.

Some neuroprosthetic devices may interact with their human host only through a small number of managed interfaces (e.g., neural connections through which signals are received and transmitted); other devices, such as those composed of biological material, may interact with the devices' host through unmanaged interfaces that may change significantly over time as a result of the growth of biological components of the device, the host's organism, or both. It may be appropriate and desirable to create outward-facing subnetworks (or “**demilitarized zones**”) that are separated physically or logically from a device's internal networks<sup>102</sup> and which interface either with the biological systems and cognitive processes of the device's human host, with supplemental prostheses or other accessories that can be connected to the device (e.g., through universal ports or sockets), with the external physical environment (e.g., to prevent sensory overload or “**sense hacking**” that could occur if the external environment supplied stimuli directly to internal systems), or with other external systems such as WiFi networks and the Internet.

#### **DENY BY DEFAULT / ALLOW BY EXCEPTION**<sup>103</sup>

The practice of denying all inbound and outbound network communications traffic by default and allowing it only after it has been approved as an exception may not be possible for some kinds of neuroprosthetic devices. For example, in the case of sensory neuroprosthetics receiving sensory stimuli from the environment, it may not be feasible or theoretically possible to apply filters or tests at the boundary between the external environment and the

---

<sup>101</sup> See the Appendix to this text for an analysis of such boundaries from a biocybernetic perspective. For an exploration of phenomenological issues, see Heersmink, “Embodied Tools, Cognitive Tools and Brain-Computer Interfaces” (2011).

<sup>102</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-188.

<sup>103</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-189.

device to determine with any accuracy what the ultimate effect of the sense data may be on the psychological health and security of the device's host and thus to allow only certain information to be transmitted inward for further processing and utilization by the device and device-host system.

#### **RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC<sup>104</sup>**

If viewed solely from the perspective of a neuroprosthetic device, **extrusion detection** is essential for preventing potentially harmful traffic from passing from the device into the biological systems or cognitive processes of the device's host. However, if viewed from the perspective of the larger device-host system, such controls are not extrusion detection but internal controls. True extrusion detection would attempt to detect and prevent, for example, the use of a neuroprosthetic device by its host or operator to conduct unauthorized denial of service attacks, the dissemination of computer viruses, worms, or malicious code, illegal surveillance, or other illicit actions targeted at external systems or individuals.

#### **PREVENT UNAUTHORIZED EXFILTRATION<sup>105</sup>**

The unauthorized **exfiltration** of information from a neuroprosthetic device or device-host system can potentially be detected and prevented through practices such as monitoring a device's communications to detect **beaconing** from within the device (e.g., directed at an external command-and-control server from which the compromised device is awaiting instructions), analyzing outgoing communications to detect **steganography**, and using traffic profile analysis to detect other anomalous communications that may potentially indicate exfiltration.<sup>106</sup> In the case of neuroprosthetic devices that control or support the cognitive processes or motor activity of their human host, care must be taken to ensure that mechanisms designed to prevent unauthorized exfiltration do not slow, block, or otherwise impede the host's communications and interaction with the external environment in a way that could result in physical or psychological harm to the host or others. In some circumstances, it may not be legally or ethically permissible to immediately block outgoing communications – even if an occurrence of ongoing unauthorized exfiltration has been confirmed – if impeding the outgoing communications could have sufficiently negative consequences, e.g., for the survival or health of the device's host.

---

<sup>104</sup> NIST SP 800-53, Rev. 4 (2013), p. F-190.

<sup>105</sup> NIST SP 800-53, Rev. 4 (2013), p. F-190.

<sup>106</sup> NIST SP 800-53, Rev. 4 (2013), p. F-190.

**PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS<sup>107</sup>**

In the case of advanced neuroprosthetic devices, unauthorized physical connections with the device (or the larger device-host system) might come not only through the connection of electronic devices to electronic components of the neuroprosthetic device but also through the presence of biological or biochemical agents and vectors (such as viruses, microorganisms, nootropic drugs, or other chemicals or substances) that can enter the host's organism and interface with biological systems.<sup>108</sup>

**PREVENT DISCOVERY OF COMPONENTS/DEVICES<sup>109</sup>**

Neuroprosthetic devices that consist largely or entirely of biological material may possess a natural ability to prevent their detection as information systems (or components of such systems) by sensors or other detection mechanisms designed to identify, locate, and analyze information systems.

**FAIL SECURE<sup>110</sup>**

It is important that advanced neuroprosthetic devices be designed to fail securely in the case of a failure of one of the device's boundary protection systems or components, however the basic concept of "secure failure" may take on a radically different form in this context. Under normal circumstances, secure failure implies that after the failure of a boundary protection device information will be unable to either enter or leave the system until the failure has been remedied. In the case of neuroprosthetic devices, the state of secure failure may require that some information be able to enter and leave the device (or device-host system) in order to avoid causing direct physical or psychological harm to a device's human host.

Hansen and Hansen argue that in general, implantable medical devices should be designed in such a way that if the entire device, individual components, or the system's security controls fail, they will "fail open" in a way that allows rather than prevents the flow of information and access to the device,

---

<sup>107</sup> NIST SP 800-53, Rev. 4 (2013), p. F-191.

<sup>108</sup> Neuroprosthetic devices that include biological components may be especially liable to such attacks. For the possibility of neuroprosthetic devices involving biological components, see Merkel et al., "Central Neural Prostheses" (2007). For a hybrid biological-electronic interface device (or "cultured probe") that includes a network of cultured neurons on a planar substrate, see Rutten et al., "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe" (2007). Hybrid biological-electronic interface devices are also discussed by Stieglitz in "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems" (2007).

<sup>109</sup> NIST SP 800-53, Rev. 4 (2013), p. F-191.

<sup>110</sup> NIST SP 800-53, Rev. 4 (2013), p. F-191-F-192.

“since it is almost always better to give possibly-inappropriate access if the alternative is death or disability [...].”<sup>111</sup> In the case of a particular advanced neuroprosthetic device, it must be carefully investigated and determined whether failing into a state that is “open” or “closed” is more likely to lead to severe harm (or even death) for the device’s host or operator under different kinds of possible circumstances. The types of information that should be allowed to enter or leave a device during failures should be determined by a device’s designer in collaboration with physicians, psychologists, and biomedical engineers who possess relevant expertise about the potential physical and psychological impacts of device failure and a loss of information flow on a device’s human host.

## Transmission confidentiality and integrity

### CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION<sup>112</sup>

Encrypting outgoing transmissions may be impossible, for example, in the case of neuroprosthetic devices that transmit information in the form of electrochemical signals that must be interpretable by natural neurons within the body of the device’s host; in such cases, the device may be required for functional and operational reasons to transmit information in a form that can be received and processed by the biological and psychological systems of the device’s host, regardless of whether that form is naturally secure. At the same time, some devices (e.g., mnemoprosthetics that are fully integrated into the holonomic storage system of a human mind<sup>113</sup>) that store and transmit information in a form that can only be processed and interpreted by the mind of the human host in whom the devices are implanted may enjoy a natural (if unconventional) form of encryption.

### CONCEAL/RANDOMIZE COMMUNICATIONS<sup>114</sup>

An adversary who is unable to gain access to the exact contents of communications may nonetheless obtain valuable intelligence by being able to observe phenomena such as the “frequency, periods, amount, and predictability” of communications.<sup>115</sup> Mechanisms or practices that conceal or obscure such patterns can contribute to the information security of a neuroprosthetic device, however the ability to randomize or conceal such communications may be limited by practical functional considerations such as the

<sup>111</sup> Hansen & Hansen, “A Taxonomy of Vulnerabilities in Implantable Medical Devices” (2010).

<sup>112</sup> NIST SP 800-53, Rev. 4 (2013), p. F-193.

<sup>113</sup> See Longuet-Higgins, “Holographic Model of Temporal Recall” (1968); Pribram, “Prolegomenon for a Holonomic Brain Theory” (1990); and Pribram & Meade, “Conscious Awareness: Processing in the Synaptodendritic Web...” (1999).

<sup>114</sup> NIST SP 800-53, Rev. 4 (2013), p. F-194.

<sup>115</sup> NIST SP 800-53, Rev. 4 (2013), p. F-194.

need to communicate effectively with the biological systems of a device's host and the fact that many kinds of communication typically utilized by a human being, and thus a device-host system (such as speech, paralanguage, and gestures), are effective precisely because they release information into an external environment in a way that is not concealed or obscured.

### Network disconnect<sup>116</sup>

The automatic termination of a neuroprosthetic device's network connection after an arbitrary predetermined period of time could potentially result in physical or psychological harm to the device's host or user if the termination occurred during a critical moment. Some naturally occurring biological cycles present within the biological systems and processes of a device's host (e.g., sleep cycles or cycles of neuronal firing) may provide opportunities for the safe deallocating and reallocating of address/port pairings, the disconnecting and reconnecting of network services, or other kinds of regular processes needed for maintaining a device's security and functionality.

### Cryptographic key establishment and management<sup>117</sup>

The need to maintain possession and confidentiality of and access to cryptographic keys that are necessary for the effective functioning of a neuroprosthetic device becomes even more critical if failure or unauthorized use of the device has the potential to cause physical or psychological harm to the device's user or others.<sup>118</sup> The **escrowing** of encryption keys may be a necessary practice but also one that must be carried out carefully – especially if a neuroprosthetic device contains components relying on use of the encryption key which, due to their implantation in the host's body, cannot easily be updated, otherwise modified, or replaced if the key should be lost or disclosed to unauthorized parties.

### Cryptographic protection<sup>119</sup>

---

<sup>116</sup> NIST SP 800-53, Rev. 4 (2013), p. F-194.

<sup>117</sup> NIST SP 800-53, Rev. 4 (2013), p. F-195.

<sup>118</sup> See Chapter Three of this text for proposed approaches to storing the cryptographic key for an implanted neuroprosthetic device on the host's body in the form of an external token, bracelet, tattoo, or other item, in order to provide device access to medical personnel in the case of a medical emergency affecting the device's host.

<sup>119</sup> NIST SP 800-53, Rev. 4 (2013), p. F-196.

When attempting to secure certain kinds of neuroprosthetic devices, it may be possible (or even necessary) to develop entirely new kinds of encryption which, for example, use the unique memories or other cognitive contents of a human mind as cryptographic keys.<sup>120</sup>

### Collaborative computing devices<sup>121</sup>

Advanced neuroprosthetic devices may be able to serve directly as collaborative computing devices; for example, an artificial eye implanted in one host could potentially stream live video that can be viewed by other persons in order to share in the host's visual experiences, or a human host possessing a body with cybernetic limbs might allow a professional dancer to take temporary control of the body in order to create a form of shared performance art. Possibilities also exist for the internal cognitive processes of neuroprosthetic devices' hosts to become collaborative computing devices by creating "hive minds" or communities of individuals whose minds are linked through their implanted neuroprosthetic devices.<sup>122</sup> A neuroprosthetic device may also allow its human host new ways of accessing, controlling, and obtaining information from traditional collaborative computing devices such as cameras, microphones, or printers. The growth of the Internet of Things and new kinds of devices such as 3D printers and smart homes creates entirely new types of networked systems that can potentially be accessed and controlled by means of neuroprosthetic devices.<sup>123</sup> All of these possibilities raise significant questions of information security both for the users and operators of neuroprosthetic devices and for other individuals who use the collaborative computing devices or can be affected by their activities.

### Mobile code<sup>124</sup>

---

<sup>120</sup> For such possibilities, see Thorpe et al., "Pass-thoughts: authenticating with our minds" (2005); Mizraji et al., "Dynamic Searching in the Brain" (2009), where the term "password" is used in a more metaphorical sense than the typical meaning in information security, but the dynamic memory searching mechanisms described could potentially also serve as the basis for an authentication system; and Gladden, "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values" (2015).

<sup>121</sup> NIST SP 800-53, Rev. 4 (2013), p. F-197.

<sup>122</sup> See Gladden, "Upgrading' the Human Entity..." (2015), and Gladden, "Cybershells, Shapeshifting, and Neuroprosthetics..." (2015).

<sup>123</sup> See Gladden, "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems" (2015), and Merkel et al., "Central Neural Prostheses" (2007).

<sup>124</sup> NIST SP 800-53, Rev. 4 (2013), p. F-198.

By virtue of their highly customized design and structure, many neuroprosthetic devices may be incapable of using common mobile code technologies (such as JavaScript and Flash animations).<sup>125</sup> Nevertheless, it is important that the designers of neuroprosthetic devices and developers of their operating systems implement adequate controls to account for the possibility that operators or hosts may attempt to install mobile code on the devices or that, for example, websites visited using a web browser or other software on a neuroprosthetic device might attempt to download and execute such code on the device.

### Architecture and provisioning for name/address resolution service<sup>126</sup>

Particularly in the case of a neuroprosthetic system that includes multiple devices implanted within a single human host that must communicate with one another,<sup>127</sup> it may be appropriate and desirable to utilize separate name and address resolution services (such as DNS servers) for processing internal information requests from the component devices that constitute the system and external information requests from external networks such as the Internet.

### Session authenticity<sup>128</sup>

Systems utilize controls that protect the authenticity of sessions in order to guard against attacks such as man-in-the-middle attacks and session hijacking.<sup>129</sup> Some kinds of neuroprosthetic devices (such as those that possess physical neural networks and interact through ongoing synaptic activity with a human host who is also a device's operator) may not utilize sessions or other commonly used control practices such as user accounts or authentication.

### Fail in known state<sup>130</sup>

Neuroprosthetic devices may be designed so that they fail (at least in the case of some kinds of failures) in a known state that preserves information

---

<sup>125</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-198.

<sup>126</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-201.

<sup>127</sup> Body area networks and body sensor networks typically constitute such systems. See Ullah et al., "A Study of Implanted and Wearable Body Sensor Network" (2008); Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012); and Li et al., "Advances and Challenges in Body Area Network" (2011).

<sup>128</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-201-F-202.

<sup>129</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-201.

<sup>130</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-202.

about the devices' final pre-failure state. It can be especially helpful for a neuroprosthetic device to be designed to fail in a known secure state in cases when an implanted neuroprosthetic device cannot easily be inspected or otherwise immediately accessed to externally determine or confirm its failure state.<sup>131</sup>

### Thin nodes<sup>132</sup>

It may be difficult to implement many kinds of neuroprosthetic devices as thin nodes, given the diverse range of complex tasks that such devices must perform; the multiple forms of communication and interaction that they may need to carry out with biological systems, other implanted devices, and external support systems; the high standards set for their functionality; and the fact that such devices may need to be engineered with a wide range of surplus capacities that may or may not ever be used (due to the difficulty of modifying devices to increase their capacities after their implantation in a human host). On the other hand, some kinds of passive neuroprosthetic devices<sup>133</sup> may function as thin nodes if they are designed to be directly controlled by the biological processes of their human host and do not need to possess sophisticated mechanisms for the storage of digital data, wireless communication, or other functionality commonly found in mobile devices.

### Honeypots<sup>134</sup>

It may or may not be feasible to provide a neuroprosthetic device itself with the components, subsystems, or subnetworks needed to create a honeypot that can either simply serve as a decoy that lures the attention of adversaries away from the device's actual core systems or which potentially allow adversaries' attacks to be observed and analyzed without creating a danger for the device's core systems. In many cases, it may not be an effective use of the limited resources that can be included in a small implantable device to create a honeypot within the device itself. Unique legal and ethical issues (including those of liability for possible damages to the host) may also arise with creating within the body of a human host such decoy systems that can attract attacks.

In some cases (e.g., those of neuroprosthetic devices that are composed largely or entirely of biological material, do not have significant mechanisms for communicating with the environment external to their human host, and

---

<sup>131</sup> See Chapter Three of this text for a discussion of issues relating to the lack of physical access to neuroprosthetic devices after their implantation.

<sup>132</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-202.

<sup>133</sup> See Chapter One of this text for a discussion of passive neuroprosthetic devices.

<sup>134</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-202.



are not easily detectable using the sort of electronic equipment that is typically used to detect and analyze mobile computers), it may be more prudent, effective, and efficient to attempt to entirely mask and conceal the device's existence than to create a honeypot which, in a sense, is purposefully designed to attract attention.<sup>135</sup>

### **Platform-independent applications<sup>136</sup>**

Typically, platforms are understood as “combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both.”<sup>137</sup> The concept of a “platform” may take on new meanings in the context of implantable neuroprosthetic devices. In some cases, the relevant “platform” may comprise an implantable mobile computer that possesses a conventional architecture and runs a common operating system like Windows, Android, or Linux. In other cases, the “platform” may consist of an electronic device in the form of a physical neural network comprising millions or billions of artificial neurons that are not capable of running an operating system or executing “programs” as traditionally understood but which may nonetheless be taught to perform certain complex patterns of behavior. In other cases, the platform may include a passive device composed of biological material or electronic components that are directly guided and controlled by the activity of the biological or cognitive processes of the device's human host; in this situation, the neuroprosthetic device provides the hardware but the platform's software is found in the body or mind of its human host. This highlights the possibility that in some cases, it may not be possible to identify or understand the “platform” created by a neuroprosthetic device simply by referring to the synthetic device itself; the platform may be constituted by or within the larger device-host system as a whole.

It is often beneficial to utilize applications that can run on multiple platforms, insofar as this enhances application portability and the possibility of running key applications on alternate platforms, in the case of some emergency that renders their primary platforms compromised or unavailable.<sup>138</sup> However, in the case of some kinds of advanced neuroprosthetic devices, it

---

<sup>135</sup> See Chapter Three of this text for proposed approaches that utilize shielding or jamming in an attempt to conceal the existence of a neuroprosthetic device.

<sup>136</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-203.

<sup>137</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-203.

<sup>138</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-203.

may not only be true that applications designed for one *type* of neuroprosthetic device will be unable to run on other types of neuroprosthetic devices, but even that applications developed for use on one neuroprosthetic implanted within a particular human being may be unable to run on other devices of the *same type* that are implanted in other human beings. Some neuroprosthetic devices may potentially store application information in biological material that shares the DNA of a device's human host and thus cannot be utilized with other human hosts; other applications may be customized to interface with the unique physical structure or cognitive processes found in the natural neural network of a particular human host and thus will not function if run on another person's device.<sup>139</sup>

### Protection of information at rest<sup>140</sup>

The phrase “**information at rest**” is generally used to describe information during those times when it is physically embodied in a particular way that is seen as relatively stable – namely, this describes “the state of information when it is located on storage devices as specific components of information systems.”<sup>141</sup> In reality, even information that is stored on physical storage devices of the most reliable and secure form imaginable is never truly “at rest,” as the physical substrates upon and within which information is stored (such as the ferromagnetic layer of a hard disk drive's platter) are continuously being impacted at the subatomic level by phenomena such as cosmic rays and probabilistic quantum effects, even if these phenomena rarely have impacts that are directly visible at the macroscopic level. In well-designed systems, this process of ongoing change at the subatomic level in the structure and composition of the substrates typically does not modify the contents of the information as it is accessed and interpreted by human beings – but it has the potential to do so. The possibility that even “information at rest” could be modified or destroyed through the impact of “soft errors” caused by cosmic rays, other electromagnetic radiation, or random quantum effects generally increases as units of data (such as bits) are stored in smaller physical structures, such as those of a single electron.<sup>142</sup>

---

<sup>139</sup> See the device ontology in Chapter Four of this text for possible ways in which a neuroprosthetic device may be customized for the unique biological structures and processes – or potentially psychological characteristics or knowledge – of a unique human host.

<sup>140</sup> NIST SP 800-53, Rev. 4 (2013), p. F-203.

<sup>141</sup> NIST SP 800-53, Rev. 4 (2013), p. F-203.

<sup>142</sup> For a discussion of various kinds of soft errors and approaches for preventing them or limiting their impact, see Borkar, “Designing reliable systems from unreliable components...” (2005); Wilkinson & Hareland, “A cautionary tale of soft errors induced by SRAM packaging materials” (2005); Srinivasan, “Modeling the cosmic-ray-induced soft-error rate in integrated circuits: an overview” (1996); and KleinOsowski et al., “Circuit design and modeling for soft errors” (2008).

For some kinds of neuroprosthetic devices that utilize biological material for storing information, new complications are added to this picture: “information at rest” that is stored within the patterns of activity of living cells (or within DNA<sup>143</sup>) may be modified or destroyed over time due to the birth, growth, mutation, or death of cells, or the alteration of DNA due to radiation, chemical agents, biological agents and vectors, or other factors.

#### **OFF-LINE STORAGE**<sup>144</sup>

For some kinds of implantable neuroprosthetic devices (e.g., those which store information within an internal physical neural network or which lack mechanisms for transmitting information to or receiving information from external systems), a device itself and its own internal storage mechanisms may constitute a form of off-line storage, insofar as the information is not accessible from any sort of external networks.

#### **Heterogeneity**<sup>145</sup>

Increasing the heterogeneity and diversity of the sources, forms, functionalities, or procedures relating to the individual components of neuroprosthetic devices, the complete devices, or larger information systems that incorporate the devices is a double-edged sword: on the one hand, such diversity “reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks.”<sup>146</sup> On the other hand, increased heterogeneity and diversity of systems and components may contravene the information security principle of utilizing conceptually simple design and may increase the cost, complexity, and difficulty of properly managing information systems.<sup>147</sup>

#### **Concealment and misdirection**<sup>148</sup>

An organization may utilize practices such as virtualization techniques, the intentional promulgation of believable but misleading information about

---

<sup>143</sup> For a discussion of the possibilities of using DNA as a mechanism for the storage of data, see Church et al., “Next-generation digital information storage in DNA” (2012).

<sup>144</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-204.

<sup>145</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-204.

<sup>146</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-204.

<sup>147</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-204.

<sup>148</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-205-F-206.

the organization's systems or operations, the concealment of system components, and **deception nets** (including **honeynets** that intentionally utilize outdated or poorly configured software ) in order to confuse adversaries and potentially lead them to undertake attacks that will be ineffective.<sup>149</sup> In the case of advanced neuroprosthetic devices, mechanisms designed for concealment and misdirection may need to be able to distinguish, for example, between an adversary who is attempting to break into and take control of a device for malicious purposes and emergency medical personnel who are attempting to “break into” and take control of a device in order to save the host from some life-threatening medical danger. In the latter case, mechanisms for concealment or misdirection purposefully added to a device or its software by their developers could potentially result in financial liability and legal and moral responsibility for the developers in the case of physical or psychological harm that is caused for the device's host or others as a result of emergency responders being actively slowed or misdirected by such mechanisms.<sup>150</sup>

### Covert channel analysis<sup>151</sup>

An organization typically identifies ways in which devices or systems emit transmissions, material objects, or other phenomena that could be used as covert channels for communication, determine the maximum bandwidth available through such covert channels for potential unauthorized communications, and attempt to reduce the bandwidth available for covert channels, insofar as this is feasible given the organization's functional needs and operational priorities.<sup>152</sup> Some kinds of neuroprosthetic devices may not only generate phenomena such as wireless transmissions, magnetic fields, electrical charges, heat, biological or biochemical substances and materials, and other objects or phenomena that can be directly observed by external parties; the devices may also stimulate the body of their human host in such a way that causes it to produce physical reactions or behaviors that can be observed by persons or sensors in the external environment and which can potentially serve as covert channels for the communication of information. It may not be legally, ethically, or practically possible to eliminate or minimize the bandwidth of all such channels.

### Information system partitioning<sup>153</sup>

---

<sup>149</sup> NIST SP 800-53, Rev. 4 (2013), p. F-206.

<sup>150</sup> See Chapter Three of this text for some proposed approaches to shielding or jamming technologies that mask or conceal a neuroprosthetic device's existence but which can be disabled by emergency medical personnel when necessary.

<sup>151</sup> NIST SP 800-53, Rev. 4 (2013), p. F-206-F-207.

<sup>152</sup> NIST SP 800-53, Rev. 4 (2013), p. F-206.

<sup>153</sup> NIST SP 800-53, Rev. 4 (2013), p. F-207.

Typical approaches to information system partitioning – such as physically separating different components in different racks within the same room, in different rooms, or in wholly different geographical locations – may not be feasible in the case of an implantable neuroprosthetic device that must be as small and compact as possible. It may be possible to physically separate components through the creation of body area networks (BANs) or body sensory networks (BSNs)<sup>154</sup> whose components are distributed throughout a host's body and interact with one another wirelessly. It may also be possible to separate the implantable device from external device or support systems that communicate with the implantable device, however care must be taken to ensure that the implanted portion of the system can continue to operate in a way that will not create the danger of physical or psychological harm for the device's host or others if the device should temporarily or permanently lose the ability to communicate with the external systems (e.g., because the device's host has entered a building whose construction blocks the transmission of wireless signals between the implanted device and external systems or components).

### Non-modifiable executable programs<sup>155</sup>

Designing an implantable neuroprosthetic device in such a way it loads and runs its operating system and applications from a storage medium that is permanently embedded within the device and which is hardware-enforced as read-only may be desirable, insofar as it helps ensure that the device's operating system and environment will not be illicitly altered or compromised by modifying the stored programs. However, the implications of such a practice must be carefully weighed. For example, it may sometimes occur that the operating system or applications contained on a device's read-only storage medium may need to be updated or upgraded in order to address vulnerabilities in the implanted versions of the programs that have become known. It may be difficult to implement such updates in situations in which it is not legally, ethically, or practically simple for the device's operator to remove or physically access the device in order to replace or alter the storage medium after the device's implantation.

---

<sup>154</sup> See Ullah et al., "A Study of Implanted and Wearable Body Sensor Network" (2008); Cho & Lee, "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks" (2012); and Li et al., "Advances and Challenges in Body Area Network" (2011).

<sup>155</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-207-F-208.

## Honeyclients<sup>156</sup>

It is theoretically possible to use neuroprosthetic devices (or their constituent components, subsystems, or subnetworks) as honeyclients that proactively explore the Internet in search of malicious code (either code designed to infect and harm a device itself or – for example, if the neuroprosthetic device is being used by cyberwarfare personnel within a military organization – designed to infect other kinds of systems which the operator of the neuroprosthetic device has an interest in protecting). However, the legal and ethical implications of such practices must be carefully considered, especially if they create an increased risk that the human host or operator of a neuroprosthetic device may experience physical or psychological damage as a result of the device’s intentional encounter with malicious code.

## Distributed processing and storage<sup>157</sup>

Some kinds of neuroprosthetic devices (such as those employing a physical neural network with holonomic or holographic storage models<sup>158</sup>) may inherently utilize distributed processing and storage.

## Out-of-band channels<sup>159</sup>

For human beings possessing certain kinds of neuroprosthetic devices, such a device may provide a new kind of “out-of-band” channel for conveying information directly to the conscious awareness or cognitive processes of its human host in a way that bypasses or avoids the traditional biologically based “in-band” channels comprising sensory organs. Conversely, for the human host of a sensory or cognitive neuroprosthetic device who ordinarily receives sensitive or secure information through the device (e.g., with information being presented in the host’s visual field through use of augmented reality or being directly incorporated into the host’s short- or long-term memory), receiving information through the use of the host’s natural biological sensory organs may constitute the use of an out-of-band channel.

## Operations security<sup>160</sup>

Operations security (or OPSEC) attempts to secure an organization’s sensitive information not directly through developing access controls for the in-

---

<sup>156</sup> NIST SP 800-53, Rev. 4 (2013), p. F-208.

<sup>157</sup> NIST SP 800-53, Rev. 4 (2013), p. F-209.

<sup>158</sup> See Longuet-Higgins, “Holographic Model of Temporal Recall” (1968); Pribram, “Prolegomenon for a Holonomic Brain Theory” (1990); and Pribram & Meade, “Conscious Awareness: Processing in the Synaptodendritic Web...” (1999).

<sup>159</sup> NIST SP 800-53, Rev. 4 (2013), p. F-209-F-210.

<sup>160</sup> NIST SP 800-53, Rev. 4 (2013), p. F-210.

formation itself but by ensuring more generally that the organization's operations do not unnecessarily disclose information that could be used by adversaries to develop more effective means of attacking the organization and obtaining the sensitive information that they ultimately wish to obtain. OPSEC carries out its work through the "(i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures."<sup>161</sup>

In the case of advanced neuroprosthetic devices, the mandate of OPSEC practices and personnel may also need to be broadened to include not only preventing the unnecessary disclosure of information about an organization's internal operations but also preventing the unnecessary disclosure of information about the personal (non-organizational) activities of members of the organization who possess neuroprosthetic devices, insofar as the sensitive organizational information contained in such devices could potentially be targeted through attacks that utilize avenues relating to members' private lives and activities.<sup>162</sup> At the same time, traditional OPSEC practices and objectives to limit the dissemination of information about the existence, purpose, use, and context of information systems may sometimes conflict with the desires of neuroprosthetic devices' human hosts, whom it may be legally and ethically difficult to prevent from disclosing information about their personal life and activities, should they desire to do so.

### Process isolation<sup>163</sup>

The use of traditional practices such as hardware separation and thread isolation may not be possible in the case of neuroprosthetic devices which, for example, utilize a physical neural network for storing and processing data.

### Wireless link protection<sup>164</sup>

#### **ELECTROMAGNETIC INTERFERENCE**

A system can potentially be protected from intentional jamming through the use of unpredictable wireless spread spectrum waveforms, while other

---

<sup>161</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-210.

<sup>162</sup> See Chapter Three for a discussion of the ways in which neuroprosthetic devices are inextricably entangled with the larger device-host system in which they operate, through integration into the neural circuitry of their human hosts.

<sup>163</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-210-F-211.

<sup>164</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-211-F-212.

technologies may provide protection against unintentional jamming or interference (e.g., from nearby devices using the same wireless frequencies).<sup>165</sup> This is especially important in the case of neuroprosthetic devices whose activity can have a critical impact on the health of their human host and whose successful functioning depends on effective wireless communication with other implanted devices or external support systems.

#### **REDUCE DETECTION POTENTIAL<sup>166</sup>**

Even if adversaries are unable to decipher the contents of messages that are being wirelessly transmitted by a particular device, simply being able to detect the existence of a device and the fact that it is transmitting signals and to potentially pinpoint the device's geolocation provides an adversary with useful information. Reducing the strength of wireless transmissions from an implanted neuroprosthetic device may reduce its detectability. Some kinds of implanted neuroprosthetic devices may already be restricted to utilizing low-power transmissions in order to avoid causing potential harm or disruptive side-effects for biological systems and material within their host's body (e.g., heat generated by the absorption of radio frequency radiation).<sup>167</sup> At the same time, transmission signal strengths must be sufficient to ensure that physical or psychological harm does not result for a device's human host due to the device's failure to execute successful wireless communications with other implanted devices or external medical support or control systems.

#### **SIGNAL PARAMETER IDENTIFICATION AND IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION<sup>168</sup>**

Some information systems may utilize "radio fingerprinting techniques" to identify and track particular devices according to the signal parameters displayed by their wireless transmissions; conversely, other devices may attempt to elicit communications from or manipulate communications with a system by intentionally imitating the signal parameters of a particular device that is already trusted by the system.<sup>169</sup> Utilizing appropriate techniques (e.g., anti-fingerprinting mechanisms employing unpredictable signal parameters) to counter such possibilities is especially important in the case of neuroprosthetic devices whose only means of communication with necessary external support and control systems is through wireless transmissions.<sup>170</sup>

---

<sup>165</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-211.

<sup>166</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-211.

<sup>167</sup> See Zamanian & Hardiman, "Electromagnetic radiation and human health: A review of sources and effects" (2005).

<sup>168</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-212.

<sup>169</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-212.

<sup>170</sup> See Chapter Three of this text for a discussion of the reliance on wireless communications that is found with many kinds of implantable neuroprosthetic devices.



## Port and I/O device access<sup>171</sup>

For implantable neuroprosthetic devices which, for some reason, are required to include physical connection ports (e.g., USB or specialized proprietary ports) or input/output devices (such as microSD card readers or specialized proprietary memory chip readers) that are accessible from the exterior of their host's body, it may be desirable from the perspective of information security to disable such devices at all times except for occasions when they are enabled through an explicit command from the device's operator or in the case of a medical emergency experienced by the device's host that causes the ports and I/O devices to be automatically enabled in order to allow for the delivery of medical treatment by emergency medical personnel.<sup>172</sup>

Note that the legal, ethical, and practical implications of such design decisions must be carefully considered: for example, if it is commonly known that a neuroprosthetic device's exterior connection ports and I/O devices will be automatically enabled in the case of particular kinds of medical emergencies experienced by the device's human host, an adversary could potentially purposefully induce a relevant kind of medical emergency for a device's host (e.g., through a physical, biological, or chemical attack or intervention) in order to gain access to fully enabled connection ports or I/O devices that the adversary can use to compromise the neuroprosthetic device.

## Sensor capability and data<sup>173</sup>

An organization's ability to restrict the activation and use of environmental sensors (such as cameras, microphones, accelerometers, GPS systems, temperature gauges, and other mechanisms) in devices belonging to the organization is a critical element of information security.<sup>174</sup>

In the case of sensory neuroprosthetics such as artificial eyes, an organization must often make a device's environmental sensing capabilities available to the device's host and operator at all times – with no delays, distortions, or other failures in service – while at the same time blocking all unauthorized parties from accessing (or potentially even knowing about the existence of) the device's sensor capacities. Adversaries who gain unauthorized access to a neuroprosthetic device's sensor capabilities could potentially use that ability

---

<sup>171</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-212.

<sup>172</sup> See Chapter Three of this text for a discussion of allowing special access to neuroprosthetic devices during health emergencies that affect their human host.

<sup>173</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-213.

<sup>174</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-213.

to conduct covert and illicit surveillance on the device's human host, the organization by whom the host is employed, other organizations or individuals with whom the host is associated, or potentially even organizations or individuals who have no direct connection with the host but whom the host happens to be passing by at the moment. In the case of cognitive neuroprosthetics, a device itself may not possess direct access to raw sense data from the environment, but it may be able to indirectly access such data through the host's memory or other cognitive processes. Motor neuroprosthetics that are used, for example, to control the movement of an artificial limb may contain accelerometers or other sensors that are intended to gather data about the position and activity of the limb but which can be utilized by adversaries to gather information about the broader physical environment, instead.

#### **PROHIBIT USE OF DEVICES<sup>175</sup>**

An organization may wish to prohibit or restrict the use of devices that possess environmental sensing or recording capabilities (such as smartphones or cameras) within particularly sensitive facilities or areas. It is one matter for an organization to deny entry to its facility to individuals possessing handheld cameras (or to require that the individuals temporarily deposit their cameras for safekeeping with the organization's personnel upon entering the facility); it is another matter to deny entry to individuals who possess certain kinds of implantable neuroprosthetic devices, such as artificial eyes that possess the same functionality as handheld cameras. In the latter case, such neuroprosthetics may, from a legal and ethical perspective, be treated as implantable medical devices, and an organization's refusal of entry or service to a person possessing such a device may in some cases be considered an unlawful form of discrimination on the basis of the person's health or medical status. Even conducting the kind of searches that may be required in order to determine the presence of some kinds of implantable neuroprosthetic devices in visitors to an organizational facility (e.g., potential customers visiting a company's retail store or showroom) may be considered an impermissibly intrusive procedure that illicitly gathers information about visitors' personal medical history and status without their express consent. Efforts by an organization to proactively jam or obstruct the functioning of some kinds of neuroprosthetic devices (such as attempts by a theater owner to prevent the use of artificial eyes to record a performance) would likely encounter legal, ethical, and practical obstacles similar to those encountered by organizations that have sought to jam the functioning of smartphones on their organizations' premises.<sup>176</sup>

<sup>175</sup> NIST SP 800-53, Rev. 4 (2013), p. F-213.

<sup>176</sup> Regarding the technological, legal, and ethical aspects of using jamming devices to block cell phone signals in places such as movie theaters and schools, see Koebler, "FCC Cracks Down on

## Usage restrictions<sup>177</sup>

Although it may be legally and ethically permissible and practically feasible for an organization to restrict the ability of its members to utilize technologies such as cameras, smartphones, printers, and scanners while in the workplace,<sup>178</sup> an organization's ability to restrict the use of such technologies by its employees during their personal, non-work time and away from workplace facilities is limited. This causes challenges for information security, insofar as the same sensitive, work-related information that was captured, generated, stored, or transmitted by neuroprosthetic devices during working hours in the workplace may also be present in or recoverable from the devices when their human hosts are away from the workplace and engaging in purely private activities.

## Detonation chambers

The ability to implement a detonation chamber (or “dynamic execution environment”)<sup>179</sup> within a neuroprosthetic device may be limited by the fact that some malicious code or applications may not be inherently (or obviously) harmful in themselves but only when allowed to interact with or be run by the cognitive processes of a particular human host. If it is not possible to simulate a host's cognitive processes with sufficient richness and accuracy in some artificial dynamic execution environment, then carrying out actions such as executing suspicious programs, opening suspicious email attachments, or visiting suspicious websites<sup>180</sup> within the detonation chamber may not reveal the harmful effects that the same actions would have when performed by a neuroprosthetic device within a particular device-host system.<sup>181</sup>

---

Cell Phone ‘Jammers’...” (2012), and Overman, “Jamming Employee Phones Illegal” (2014).

<sup>177</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-214.

<sup>178</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-214.

<sup>179</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-214.

<sup>180</sup> *NIST SP 800-53*, Rev. 4 (2013), p. F-214.

<sup>181</sup> Practical difficulties with implementing a detonation chamber within a neuroprosthetic device itself could arise either from the nature of the device's computing platform (e.g., it may be difficult or impossible to implement such an environment within a neuroprosthetic device that does not execute traditional programs but instead processes information using a physical – and perhaps biological – neural network) or simply from limitations to the processing power, storage capacity, or power supply of a device's internal computer. See the device ontology in Chapter Four of this text for a discussion of such considerations.

Part IV

## **Appendix**

## Appendix

# Biocybernetic Classification of Advanced Neuroprosthetic Devices

### Summary

One way of classifying neuroprosthetic devices is according to the neural processes of their human hosts in which they participate or to which they are linked.<sup>1</sup> Here “neural processes” are defined broadly to include both the physical processes of sense-data reception that lead directly to perception in the mind as well as the actuation of physical actuators and organs that follows directly from mental activity such as volition (or potentially from the semi-mental activity of reflexes). It is possible to classify neural processes at a very general level or to define the more specific subprocesses that constitute each process.

### Cybernetic implications

The neural processes in which a neuroprosthetic device participates are relevant from a cybernetic perspective because many of the processes are essential elements of the hostmind’s control, communication, and connectivity with regard to its own body, to concrete organizations and supraystems in which it participates, in its relation to other minds, and in its relation to the environment as a whole. The fact that a neuroprosthetic device participate in neural processes has broad potential to create, radically modify, or suppress its host’s processes of communication, connectivity, and control.

---

<sup>1</sup> See Chapter One of this text and the device ontology in Chapter Four for discussions of different ways in which neuroprosthetic devices can be integrated into the neural circuitry of a human host.

## Importance for information security

The processes in which a neuroprosthetic device participates are relevant from an information security perspective because many of the neural processes are either directly involved with the acquisition, storage, retrieval, and use of some of the most confidential and intimate kinds of information relating to a human mind or have the potential to indirectly enhance, alter, or disrupt those processes.<sup>2</sup>

## Classification of neuroprosthetic devices by neural process

Neuroprosthetics can be classified according to whether they participate in the *sensory*, *cognitive*, or *motor* neural processes of their human host.<sup>3</sup> Below we consider in more detail these three kinds of neuroprosthetic devices. Note that a single device may participate in many of the processes described below; the descriptions are thus generally not mutually exclusive.

### Sensory neuroprosthetic devices

A sensory neuroprosthetic device is an implant or other system that participates in the acquisition of sense data from distal stimuli, its mapping or translation into a modality that the device's hostmind can receive and interpret, or the transmission of the proximal stimuli to the point of their reception at the hostmind's interface with the sensory organs. Sensory neuroprosthetics can be described according to the particular stage within the process of sensing in which they participate and according to the relationship that they create between sense data, sensory organs, and sense modalities. Below we consider these kinds of sensory neuroprosthetic devices in more detail.

#### **SENSORY NEUROPROSTHETICS DESCRIBED BY THE STAGE WITHIN THE PROCESS OF SENSING IN WHICH THEY PARTICIPATE**

Sensory neuroprosthetics can participate in the mind's activity of sensing by serving as **receptors** that register some kind of action or object, as **transmitters** that carry sense data from its original receptor toward the hostmind and its processes of conscious awareness or unconscious processing, or as **presenters** that make sense data available to the brain, either to the hostmind's conscious perception or for the autonomous regulation of biological processes. Below we consider these three ways in which neuroprosthetics can participate in processes of sensing.

---

<sup>2</sup> See Chapter Two of this text for an overview of general principles of information security and Chapter Three for the unique challenges of providing information security for advanced neuroprosthetic devices.

<sup>3</sup> See Chapter One of this text for additional discussion of these different kinds of neuroprosthetic devices.

### *The neuroprosthetic device as receptor*

Neuroprosthetics that constitute or possess receptors register particular kinds of activity or the presence of certain kinds of material objects and carry out sensory transduction to convert the received energy into signals that can be transmitted either to neurons (e.g., as electrochemical signals) or other devices (e.g., as digital data). Such receptors may take several forms.

#### ELECTROMAGNETICALLY RECEPTIVE NEUROPROSTHETICS

An electromagnetic receptor registers electromagnetic radiation, a magnetic field, or electric charge. Neuroprosthetics incorporating such elements include:

- **Photoreceptive neuroprosthetics**, which register electromagnetic radiation (typically from the environment external to the hostmind's body) by detecting photons. In a natural human being, this system comprises photoreceptors in the retina. An implant may register light that falls within the spectrum naturally visible to human beings or it may register electromagnetic radiation of a frequency higher than that of visible light (e.g., ultraviolet light, X-rays, or gamma rays) or lower than that of visible light (e.g., infrared light or radio waves). Existing kinds of retinal implants are typically photoreceptive neuroprosthetics.<sup>4</sup>
- **Electroreceptive neuroprosthetics**, which register the presence of an electric charge, either in the form of static electricity or an electric current. In a natural, unaugmented human being, sensory and motor neurons can be indiscriminately stimulated by electricity, however human beings do not have specialized electroreceptors.<sup>5</sup>
- **Magnetoreceptive neuroprosthetics**, which register the presence of a magnetic field. It is not clear whether natural human beings possess such a system; the supposed existence of magnetosensitive bones or brain cells is a matter of ongoing debate.<sup>6</sup>

---

<sup>4</sup> See Linsenmeier, "Retinal Bioengineering" (2005); Weiland et al., "Retinal Prosthesis" (2005); and Viola & Patrinos, "A Neuroprosthesis for Restoring Sight" (2007).

<sup>5</sup> Note that electroreceptors are not limited to detecting naturally occurring electric current or electric fields present in an environment. For example, a neuroprosthetic device could be said to possess "electroreceptors" of a particular sort if it includes a mini-stereo audio input port or a power supply input port into which an AC or DC power cable can be inserted to charge the device's internal battery.

<sup>6</sup> In the case of neuroprosthetic devices, the detection of magnetic fields could be used, for example, in a specialized way to detect the presence of an external hardware token that provides access to the device; see Chapter Three of this text for a discussion of such tokens.

## MECHANORECEPTIVE NEUROPROSTHETICS

A mechanoreceptor registers physical force, motion, or pressure. Neuroprosthetics incorporating such elements include:

- **Audioceptive neuroprosthetics**, which contain a specialized form of mechanoreceptor that registers sound waves either from the environment external to the hostmind's body or from inside the body. In a natural human being, this system includes hair cells in the ear. Such a receptor may register sound frequencies and volumes detectable by the human ear or sound waves possessing higher or lower frequencies or at a lower volume than the ear can naturally detect. Existing models of cochlear implants and auditory brainstem implants are typically audioceptive neuroprosthetics.<sup>7</sup>
- **Tactioceptive neuroprosthetics**, which contain a specialized form of mechanoreceptor that registers pressure from objects or phenomena – typically external to the host's body – that are physically touching the receptor, either with a level of force that falls within the spectrum of what is normally perceivable by human beings through tactioception or with a greater or lesser degree of sensitivity. In a natural human being, this system includes mechanoreceptors in the somatosensory system, including in the skin, muscles, and bodily organs. Existing kinds of bidirectional sensorimotor robotic prosthetic hands often utilize such mechanisms to detect pressure applied to or by the device's fingers.<sup>8</sup>
- **Proprioceptive neuroprosthetics**, which contain a specialized form of mechanoreceptor that registers the internal pressure and force exerted and experienced by limbs and other components of the hostmind's body depending on their current position. In a natural human being, this system includes mechanoreceptors in the skeletal striated muscles and joints.
- **Equilibrioceptive neuroprosthetics**, which contain a specialized form of mechanoreceptor that registers the orientation of gravitational force exerted on the implant (and thus typically the direction toward the ground). In a natural human being, this system includes hair cells and vestibular nuclei in the ears.
- **Thermoceptive neuroprosthetics**, which contain a specialized form of mechanoreceptor that registers the kinetic energy of the receptor or matter adjoining it. (Note that this would not include a device utilizing the remote thermometric technique of pyrometry.) In a natural

<sup>7</sup> See Cervera-Paz et al., "Auditory Brainstem Implants: Past, Present and Future Prospects" (2007).

<sup>8</sup> For example, see Hoffmann, "Introduction to Neuroprosthetics" (2011), pp. 792-93.



human being, there are different thermoreceptors specialized to detect heat and cold.

- **Nociceptive neuroprosthetics**, which contain a specialized form of mechanoreceptor that registers an “excessive” level of pressure or physical force that is likely to prove harmful or destructive to the host-mind’s body and that, in a natural human being, is perceived through the modality of pain. In some circumstances such a device may alternatively utilize chemoreceptors rather than mechanoreceptors. In a natural human being, this system involves nociceptors in the somatosensory system, including in the skin, muscles, and bodily organs.

#### CHEMORECEPTIVE NEUROPROSTHETICS

A chemoreceptor registers the presence of particular kinds of chemical substances, typically on the basis of their molecular structure. Neuroprosthetics incorporating such elements include:

- **Gustatory neuroprosthetics**, which contain a specialized form of chemoreceptor that registers the presence of particular chemical substances dissolved in a liquid medium. In a natural human being, this system includes chemoreceptors of the taste buds, the tongue, and certain associated cranial nerves.
- **Olfactory neuroprosthetics**, which contain a specialized form of chemoreceptor that registers the presence of particular airborne chemical substances. In a natural human being, this system includes chemoreceptors of olfactory receptor neurons, the olfactory bulb, nose, and the olfactory nerve.
- **Interoceptive neuroprosthetics**, which contain a specialized form of chemoreceptor that registers the presence of particular chemical substances in the body that directly or indirectly indicate the status of specific biological processes or systems that are typically perceived through the modality of interoception in the form of hunger, thirst, drowsiness,<sup>9</sup> etc. In a natural human being, this system comprises chemoreceptors (as well as mechanoreceptors) in various bodily organs and systems.

#### CHRONOCEPTIVE NEUROPROSTHETICS

A chronoceptive implant registers the passage of time in a way that either is typically perceived by the hostmind through the modality of chronoception

---

<sup>9</sup> For the possibility of neuroprosthetic devices that relate to their host’s need for or experience of sleep, see Claussen & Hofmann, “Sleep, Neuroengineering and Dynamics” (2012), and Kourany, “Human enhancement: Making the debate more Productive” (2013), pp. 992-93.

or is used to regulate biological processes. In a natural human being, this role is performed by systems including the cerebral cortex, cerebellum, and basal ganglia.<sup>10</sup>

#### XENOCEPTIVE NEUROPROSTHETICS

A xenoceptive neuroprosthetic device registers the presence of some activity, phenomenon, or material object other than those mentioned above and which are not typically perceived by the hostmind of a natural human being. Examples would be devices that can register ultrasound, X-rays, infrared light, or the presence of chemicals that the human nose and tongue cannot detect. Such a device can be said to perform “xenoception.”

##### *The neuroprosthetic device as transmitter*

Some neuroprosthetics transmit those signals that have been generated after a proximal stimulus has undergone sensory transduction (either by receptor neurons or a prosthetic device) and has been converted either into a pattern of electrochemical activity that can be transmitted to other neurons or a digital representation of such activity that can be transmitted through artificial components. A transmitter moves sense data away from the original receptor and toward perception by the hostmind.

##### *The neuroprosthetic device as presenter*

A neuroprosthetic device can make sense data available to the host’s brain, which may entail the data being consciously perceived by the host’s mind or being used without conscious awareness for the autonomous regulation of biological processes. Such a device typically presents data in the form of neural signals or activity that are delivered to the part of the host’s brain that serves as an interface with the relevant sensory system. A neuroprosthetic device that presents sense data to the host’s conscious awareness or autonomous neural systems in a way that can be utilized can take several forms:

- **Ophthalmoesthetic neuroprosthetics**, which present data to a hostmind through its naturally existing modality of vision. The sense data presented may be sense data that was received from the environment in the form of light, virtual data representing the “light” received in a virtual environment, or other sense data that has been remapped to the modality of vision.<sup>11</sup> In a natural human being, this system includes the optic nerve and regions of the brain such as the visual cortex.

---

<sup>10</sup> For a discussion of biological timekeeping mechanisms that are employed by living organisms at the intracellular and intercellular level to maintain both relatively short ultradian rhythms (which primarily regulate an organism’s internal intracellular processes) and longer circadian rhythms (which primarily regulate an organism’s interaction with its external environment), see Lloyd, “Biological Time Is Fractal: Early Events Reverberate over a Life Time” (2008).

<sup>11</sup> Regarding the possibility of sensory substitution, see Wiener, *Cybernetics* (1961), loc. 2784ff;

- **Audioesthetic neuroprosthetics**, which present data to a hostmind through its naturally existing modality of hearing. The sense data presented may be sense data that was received from the environment in the form of sound, virtual data representing the “sound” received in a virtual environment, or other sense data that has been remapped to the modality of hearing. In a natural human being, this system includes the cochlear nerve and auditory cortex.
- **Gustatoesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of taste. The sense data presented may be sense data that was received from the environment in the form of taste, virtual data representing the “taste” received in a virtual environment, or other sense data that has been remapped to the modality of taste. In a natural human being, this system includes certain cranial nerves and the gustatory cortex.
- **Olfactoesesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of smell. The sense data presented may be sense data that was received from the environment in the form of smell, virtual data representing the “smell” received in a virtual environment, or other sense data that has been remapped to the modality of smell. In a natural human being, this system includes the olfactory bulb and olfactory cortex.
- **Tactioesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of touch. The sense data presented may be sense data that was received from the environment in the form of touch, virtual data representing the “touch” received in a virtual environment, or other sense data that has been remapped to the modality of touch. In a natural human being, this somatosensory system includes many sensory receptors and the primary somatosensory area in the parietal lobe.
- **Proprioesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of (either conscious or unconscious) proprioception. The sense data presented may be sense data that was received from the body, virtual data representing the internal status or processes of the hostmind’s “body” in a virtual environment, or other sense data that has been remapped to the modality of propri-

oception. In a natural human being, this system includes sensory neurons in the inner ear and ligaments as well as the cerebrum and cerebellum.

- **Equilibrioesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of balance. The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to the orientation of the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of balance. In a natural human being, this function is filled through joint action of the vestibular system (including the inner ear, cerebellum, and thalamus), visual system, and proprioceptive system.
- **Thermoesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of temperature. The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to the temperature of the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of temperature. In a natural human being, this system includes portions of the thalamus.
- **Nocioesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of pain. The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to the pain of the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of pain. In a natural human being, this system includes nociceptors and portions of the brain stem.<sup>12</sup>
- **Interoesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modalities of interoception (e.g., hunger or thirst). The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to phenomena of the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modalities of interoception. In a natural human being, this system includes various internal organs and regions of the brain.
- **Chronoesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of time perception. The sense data presented may be sense data that was received from the body,

---

<sup>12</sup> For different kinds of neuroprosthetic devices that have an analgesic effect of reducing the experience of pain or producing a feeling of euphoria for their human host, see Denning et al., "Neurosecurity: Security and Privacy for Neural Devices" (2009).

virtual data received from or corresponding to the passage of time experienced by the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of time perception. In a natural human being, this system includes parts of the brain such as the cerebral cortex, cerebellum, and basal ganglia.

- **Echoesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of acoustic wayfaring (or echolocation). The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to the wayfaring of the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of echolocation. To the extent that such a system exists in natural human beings, it may include both the cochlear nerve and auditory cortex as well as the visual cortex.
- **Magnetoesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of magnetoreception. The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to virtual magnetic fields experienced by the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of magnetoreception. In a natural human being, the existence of such a system is a controversial hypothesis; if it exists, it may include magneto-sensitive bones or cells in the brain.
- **Electroesthetic neuroprosthetics**, which present data to the hostmind through its naturally existing modality of electroreception. The sense data presented may be sense data that was received from the body, virtual data received from or corresponding to a virtual electric charge experienced by the hostmind's "body" in a virtual environment, or other sense data that has been remapped to the modality of electroreception. In a natural human being, this does not exist as a true sensory modality; the human hostmind can experience electrical charge in a gross way if sensory and motor neurons are indiscriminately stimulated by a sufficiently large external electrical charge. Some animals have a dedicated system for electroreception.

#### **ACCORDING TO RELATIONSHIP OF SENSE DATA, SENSORY ORGAN, AND SENSE MODALITY**

It is possible for a neuroprosthetic device to participate in (and help create) a process that mimics those found in unaugmented human beings – e.g., a process in which light is received by the photoreceptors in an eye, which

then transmits the sense data to the brain, where it is perceived by the mind through the modality of vision. However, the possibility of using neurocybernetic systems to alter or “remap” the normal processes of sensing date back at least as far as the 1940s, when Norbert Wiener considered the possibilities, for example, of rerouting visual sense data received by our eyes so that it would be perceived by our mind through our sense modality of hearing, or rerouting auditory sense data received by our ears so that it would be perceived by our mind through our sense modality of vision.<sup>13</sup> Below we consider several different ways in which a sensory neuroprosthetic device can tie together sense data with a sensory organ and sense modality to create a unified process of sensing for its human host.

#### ***Orthoesthetic neuroprosthetics***

An orthoesthetic neuroprosthetic device participates in a process in which the presence of some activity or object (either in the environment external to the host’s body or within the host’s body) that is typically registered by the hostmind’s natural organic sensory organs and perceived by the hostmind is registered and transmitted to the hostmind using the same sense modality that is normally used by the natural sensory organs. For example, an artificial eye that registers the arrival of photons from the external environment and converts this stimulus into sense data that is transmitted through the optic nerve to the brain where it is interpreted by the mind through the sense modality of vision would be *orthoesthetic*.

#### ***Xenoceptive neuroprosthetics***

As described above, a xenoceptive neuroprosthetic device registers the presence of some activity or object (either in the environment external to the host’s body or within the host’s body) that is not typically registered by the host’s natural organic sensory organs. This means that, by definition, the artificial (or at least augmented) organs used to register such sense data differ from those of normal human beings. It also means that the mind does not have a “natural” or default sense modality through which to consciously perceive such data; the designer of the device must decide which modality will be used for that purpose.

#### ***Xenesthetic neuroprosthetics***

A xenesthetic neuroprosthetic device is an implant that presents sense data to the hostmind through a modality that has been newly fashioned, made possible, or unlocked by the implant and which is not one of the sense modalities naturally present in, available to, and used by the hostmind.

---

<sup>13</sup> See Wiener, *Cybernetics* (1961), loc. 2784ff. For more recent discussions, see Lebedev, “Brain-Machine Interfaces: An Overview” (2014), p. 106, and Warwick, “The cyborg revolution” (2014).

***Xenosensory neuroprosthetics***

Together, we can describe xenoceptive and xenesthetic neuroprosthetic devices as “*xenosensory*” neuroprosthetics that allow their human host to either detect and experience alien forms of stimuli or to experience stimuli in alien ways.

***Alloesthetic neuroprosthetics***

An alloesthetic neuroprosthetic device is an implant that presents to the hostmind through one modality sense data that is normally perceived by the hostmind through another modality (or which is not normally perceived by the hostmind at all).<sup>14</sup>

***Exoesthetic neuroprosthetics***

An exoesthetic device presents sense data that relate to the environment external to the host’s body using sense modalities that normally relate to phenomena occurring within the host’s body. For example, an implant that registers ultrasound waves and maps them so that they are perceived by the host through his or her modality of proprioception would be *exoesthetic* (as well as being xenoceptive and *xenosensory*).

***Endoesthetic neuroprosthetics***

An endoesthetic device presents sense data that relate to the host’s own body (and especially its internal functions) using a sense modality that normally conveys information about the external environment. For example, an implant that maps data about one’s body temperature to a heads-up display presented through augmented vision would be *endoesthetic*. This is similar to forms of exteroception seen in animals such as the octopus.

**Cognitive neuroprosthetic devices**

A cognitive neuroprosthetic device participates in or supplements processes that are internal to the hostmind and which do not directly involve either sensory organs or motor organs (although the processes may receive input from or transmit output to such organs).

**ACCORDING TO THE LEVEL OF CONSCIOUS INTERFACE**

Cognitive neuroprosthetic devices can be described according to whether the device’s action directly affects and is experienced by the user’s conscious awareness. A device may act on both levels simultaneously.

---

<sup>14</sup> The examples discussed by Wiener would constitute alloesthetic neuroprosthetic devices; see Wiener, *Cybernetics* (1961), loc. 2784ff.

***With the host's conscious awareness***

A cognitive neuroprosthetic device may participate in or supplement processes that are internal to the hostmind and which are experienced by, constitute, inform, or are controlled by the hostmind's conscious awareness. An example would be a mnemoprosthetic device that stores memories and allows the user to recall and consciously experience the memories through an act of will.<sup>15</sup>

***Without the host's conscious awareness***

A cognitive neuroprosthetic device may integrate with the neural circuitry of its human host without the device's activity being directly experienced as such or controlled by the hostmind's conscious awareness. Some kinds of deep brain stimulation devices may be such a form of technology.<sup>16</sup>

**ACCORDING TO THE DEVICE'S ROLE IN COGNITIVE PROCESSES**

One can classify cognitive neuroprosthetics according to the role that they play in their host's cognitive processes. Some cognitive neuroprosthetics relate primarily to the contents of cognitive processes; others relate to the hostmind's manner or quality of experiencing reality; and still others relate to the hostmind's processes of deciding, acting, executing, or instructing. Below we consider these possibilities.

***Relating to the contents of cognitive processes***

An implant may participate in or supplement the hostmind's cognitive processes in a way that relates primarily to the stable (long-term) or volatile (short-term) contents that provide the objects and raw building materials for use in the hostmind's active cognitive processes. Such devices may include:

- **Mnemoprosthetics**, which participate in or supplement the hostmind's processes of memory encoding, storage, or retrieval. They may be involved with short-term memory, long-term memory, or the hostmind's almost instantaneous processes of iconic, echoic, and haptic sensory memory (which only in a limited sense involves encoding, storage, and retrieval).<sup>17</sup>

<sup>15</sup> For discussion of neuroprosthetic devices that allow "playback" of recorded or previously experienced information, see Merkel et al., "Central Neural Prostheses" (2007); Robinett, "The consequences of fully understanding the brain" (2002); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>16</sup> See Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011), and Berg, "Pieces of Me: On Identity and Information and Communications Technology Implants" (2012).

<sup>17</sup> For the possibility of developing mnemoprosthetics, see Han et al., "Selective Erasure of a Fear Memory" (2009), and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).



- **Personality-related neuroprosthetics**, which participate in or supplement the hostmind's processes relating to the long-term formation, storage, and manifestation of personality traits.<sup>18</sup>
- **Emotional neuroprosthetics**, which participate in or supplement the hostmind's processes relating to the long-term development of emotional patterns and immediate influence of current emotional states on behaviors.<sup>19</sup>
- **Belief-related neuroprosthetics**, which participate in or supplement the hostmind's processes relating to belief. Such devices may relate either to the long-term formation, storage, and retrieval of and reliance on convictions and long-lasting beliefs or to the short-term (almost instantaneous) formation, storage, and retrieval of and reliance on immediate and reflexive beliefs or assumptions about the surrounding environment or state of the hostmind's body that are based on real-time sensory input.
- **Perceptual neuroprosthetics**, which participate in or supplement the hostmind's processes relating to the formation, experiencing, and use of sensory perception. Such devices relate to percepts that are comprehended by the hostmind as the final stage of the process of perception rather than to the raw sense data that is found in chronologically prior processes (in which case the devices would be sensory rather than cognitive neuroprosthetics).<sup>20</sup>
- **Sketchpad-related neuroprosthetics**, which participate in or supplement the hostmind's processes relating to the formation, experiencing, and use of contents of the hostmind's visuo-spatial sketchpad (as described in the Working Memory model<sup>21</sup>), which is similar to the imagination but involves real sense data and perceptions rather than imagined and artificially produced images; it is the unified experience of one's state and surroundings that draws on sense data and real-time

---

<sup>18</sup> For the possibility of developing personality-related neuroprosthetics, see Soussou & Berger, "Cognitive and Emotional Neuroprostheses" (2008).

<sup>19</sup> For the possibility of developing emotional neuroprosthetics, see Soussou & Berger, "Cognitive and Emotional Neuroprostheses" (2008); Hatfield et al., "Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior" (2009); Kraemer, "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation" (2011); and McGee, "Bioelectronics and Implanted Devices" (2008), p. 217.

<sup>20</sup> Many kinds of neuroprosthetic devices relating to sensory perception already exist; see Lebedev, "Brain-Machine Interfaces: An Overview" (2014); Merkel et al., "Central Neural Prostheses" (2007); and others for an overview.

<sup>21</sup> E.g., see Baddeley, "The episodic buffer: a new component of working memory?" (2000).

percepts and is something that is more reflexively produced and experienced than consciously controlled.

***Relating to the quality and experience of cognitive processes***

A neuroprosthetic device may affect the hostmind's *manner* or *quality* of experiencing reality rather than directly selecting the objects of experience. Such devices may include:

- **Consciousness-related neuroprosthetics**, which affect the quality and nature of the hostmind's experience consciousness and self-awareness rather than providing or choosing the objects of conscious awareness.
- **Hypnoprosthesis**, which participate in or supplement the hostmind's shift into or out of an unconscious "dream-state," the experience of that state, or the specific contents of what is "dreamt of."<sup>22</sup> In a sense, a general anesthetic or intoxicant fills a similar role. Such neuroprosthetics may affect the hostmind's processes of entering, experiencing, exiting, or avoiding sleep.
- **Attention-related neuroprosthetics**, which participate in or supplement the hostmind's experiencing of the quality of attentiveness and attention that is focused on one particular thing (or range of things). It relates to the sort of "metacognition" that is used by the mind to correct one's wandering, wayward attention.

***Relating to processes of deciding, acting, and instructing***

A neuroprosthetic device may participate in or supplement the hostmind's processes of deciding, acting, executing, or instructing. Such devices may include:

- **Episodic-buffer-related neuroprosthetics**, which participate in or supplement the hostmind's processes of creating unified, ordered units of visual, spatial, and verbal information from disparate sense data and percepts. In the Working Memory model, this function is performed by the "episodic buffer," which is connected to long-term memory.<sup>23</sup> Its work is largely executed autonomously and subconsciously.
- **Ideational neuroprosthetics**, which participate in or supplement the hostmind's processes of generating (or attempting to generate) new ideas or imaginings. While some of its activities happen subconsciously, "behind the scenes," it can be consciously directed in an effort to generate certain kinds of new ideas.

<sup>22</sup> For the possibility of neuroprosthetic devices relating to sleep, see Claussen & Hofmann, "Sleep, Neuroengineering and Dynamics" (2012), and Kourany, "Human enhancement: Making the debate more Productive" (2013), pp. 992-93.

<sup>23</sup> See Baddeley, "The episodic buffer: a new component of working memory?" (2000).

- **Inner-monologue-related neuroprosthetics**, which participate in or supplement the hostmind's processes of carrying out an internal monologue – either for purposes of conceptualizing and formulating speech to be verbally articulated for sharing with others or for purposes of reasoning internally and attempting to arrive at some reasoned conclusion.
- **Metavolitional neuroprosthetics**, which participate in or supplement the hostmind's processes of metavolition, which involves forming, storing, and drawing on volitions *about* the hostmind's volitions – e.g., forming a desire to change one's personal habits or preferences. This is closely tied to the notion of conscience.<sup>24</sup>
- **Volitional neuroprosthetics**, which participate in or supplement the hostmind's processes of volition, which involves forming, storing, and drawing on volitions that combine a desire and a belief.<sup>25</sup>
- **Habit-related neuroprosthetics**, which participate in or supplement the hostmind's processes of forming, storing, and drawing on subconscious habits or preferences of which the hostmind may not be aware.
- **Autonomous cognitive neuroprosthetics**, which participate in or supplement the hostmind's processes of receiving, processing, and responding to sense data from the hostmind's body and the environment in ways over which the hostmind has no conscious control and of which it may not have any conscious awareness. This often involves the autonomous or reflexive regulation of internal neurological or psychological processes.<sup>26</sup>

## Motor neuroprosthetic devices

Some motor neuroprosthetics device participate in the process that occurs at the point of the hostmind's interface with the motor system of translating a volition or reflexive mental instruction into a stimulus that activates or informs the functioning of transmission mechanisms that carry instructions to

---

<sup>24</sup> See Negoescu, "Conscience and Consciousness in Biomedical Engineering Science and Practice" (2009), and Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

<sup>25</sup> For a discussion of the nature of volition (and its relationship to conscience and moral responsibility), see Calverley, "Imagining a non-biological machine as a legal person" (2008).

<sup>26</sup> If a neuroprosthetic device is involved with regulating biological processes such as breathing, digestion, or circulation, it may be more likely to be a motor neuroprosthetic device rather than a cognitive neuroprosthetic device. The device's classification depends on the nature of the output or impact produced by the device and the system upon which it acts.

the motor plants or actuators that will ultimately manifest the motor action. Other motor neuroprosthetics carry out the actual transmission of such instruction-bearing stimuli to a motor plant or actuator (in the human organism, typically via a neuroeffector junction) or the interpretation of instructions and execution of the intended action by the motor plant, motor organ, or actuator. Such devices can be classified according to the particular motor modality with which they are associated or according to the relationship that they facilitate between motor instructions, a motor organ, and a motor modality.

#### ACCORDING TO THE PARTICULAR MOTOR MODALITY UTILIZED

Motor neuroprosthetics can be classified according to the particular motor modality that they employ. For example, using one's legs to walk across a room and using one's hands to play a musical instrument both involve similar kinds of motor action if viewed at the microanatomical level of muscles being electrically stimulated by the motor neurons that innervate them, however each kind of action has a different purpose and constitutes a different sort of conscious experience, from the perspective of the person performing these actions. Different kinds of motor neuroprosthetics include:

- **Logopoietic or symbolic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of language, whether oral or written and whether utilizing a natural human language or some synthetic language. These include:
  - **Rhetopoietic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of *oral verbal language*, whether expressed via a physical voicebox in a natural environment or as virtual oral speech within a virtual environment.
  - **Glyptopoietic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of *written verbal language*, whether expressed via writing or typing words in a natural physical environment or as virtual text visible within a virtual environment or other forms of digital text that can be stored and transmitted by computer. This also includes expression using sign language or other modalities in which words or letters are "written" using a symbolic form that must be presented and accessed visually.
  - **Mythopoietic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of a natural (as opposed to synthetic) human language, whether expressed orally or in written form and in physical or virtual venues.
  - **Synthologopoietic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of an artificial (as opposed to natural human) language, whether expressed orally or in written

form and in physical or virtual venues. Such a language may be an artificial language that is shared by human beings and synthetic entities that can be expressed in oral speech or a language using symbols, icons, or other forms (perhaps three-dimensional) that can only be expressed and represented with the aid of particular technologies. If such symbolic languages can only be expressed or interpreted by a particular human mind (or group of minds that are related in some way) then they could potentially be used as an encryption mechanism or method for user authentication.<sup>27</sup>

- **Anothological motor neuroprosthetics**, which express volitions or reflex instructions using the modality of a hypothesized language of (pure) thought<sup>28</sup> that is used internally by human minds to conceptualize ideas before translating them into natural human language. It is unclear to what extent such a language of pure thought exists and, if it does exist, to what extent it can be said to be identical (or different) for each human being; it is also unclear to what extent it could be expressed using either synthetic or virtual actuators – given the fact that, by definition, in its normally occurring form it is not directly expressed through motor activity and never otherwise exists outside of a mind’s internal cognitive processes. If such devices can in fact be constructed, they might thus be better classified as anothological *cognitive* neuroprosthetics rather than motor neuroprosthetics.
- **Nonsymbolic motor neuroprosthetics**, which express volitions or reflex instructions using modalities that do not include written or spoken symbols. These include:
  - **Paralinguistic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of paralanguage (such as tone of voice) and the motor organs of a natural, synthetic, or virtual voicebox.

---

<sup>27</sup> See Thorpe et al., “Pass-thoughts: authenticating with our minds” (2005).

<sup>28</sup> For just a small sampling of the many debates that touch on such issues, see, e.g., Braddon-Mitchell & Fitzpatrick, “Explanation and the Language of Thought” (1990); Clark, “Systematicity, Structured Representations and Cognitive Architecture: A Reply to Fodor and Pylyshyn” (1991); Smolensky, “The Constituent Structure of Connectionist Mental States: A Reply to Fodor and Pylyshyn” (1991); Cory, “Language, Brain, and Neuron” (2000); Taylor & Taylor, “The Neural Networks for Language in the Brain: Creating LAD” (2003); and Katz, “The Hypothesis of a Genetic Protolanguage: An Epistemological Investigation” (2008).

- **Oculesic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of oculesics and the motor organs of natural, synthetic, or virtual eyes or visual organs.
- **Kinesic motor prosthetics**, which express volitions or reflex instructions using the modality of facial expressions, gestures, posture, or gross manipulation as manifested through the motor organs of a natural, synthetic, or virtual face or body.
- **Haptic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of touch and fine manipulation and the motor organs of a natural, synthetic, or virtual body.
- **Proxemic motor neuroprosthetics**, which express volitions or reflex instructions using the modality of locomotion, relocation of the hostmind's body, and a change of inhabited environment, produced through the motor organs of a natural, synthetic, or virtual body.
- **Organ-related motor neuroprosthetics**, which express either conscious volitions, subconscious desires, or autonomous reflex instructions through biological processes such as heart rate, blood chemistry, digestion, and breathing that are affected by the organs of a natural, synthetic, or virtual body.<sup>29</sup>

#### **ACCORDING TO RELATIONSHIP OF MOTOR INSTRUCTIONS, MOTOR ORGAN, AND MOTOR MODALITY**

Motor neuroprosthetics can be classified according to the relationship that they create (or support) between a particular kind of motor instruction generated in their host's brain, the motor modality (such as speech or motion) through which the instructions will be expressed, and the kind of motor organ (whether a natural or robotic limb, natural or artificial voicebox, or computer administrating a virtual reality environment) by and through which the modality will ultimately be physically expressed. Some kinds of motor neuroprosthetics may create relationships similar to those found in natural human beings – e.g., if instructions from the brain to contract certain muscles in one's legs are expressed through the modality of locomotion as physically manifested by natural or synthetic muscles in one's legs. Other kinds of motor neuroprosthetics may create relationships quite different from those found in natural human beings – e.g., if a host's volition to orally pronounce the word “walk” is detected by a neuroprosthetic device which expresses the instruction not through the modality of speech but through the

<sup>29</sup> For discussion of such neuroprosthetic devices that affect the internal biological processes of their human host, see McGee, “Bioelectronics and Implanted Devices” (2008), p. 209, and Gasson, “Human ICT Implants: From Restorative Application to Human Enhancement” (2012), pp. 12-16.

modality of locomotion, and not by stimulating muscles in the host's natural legs but by moving the legs of the avatar within a computer game or virtual reality environment. Different kinds of motor neuroprosthetics include:

- **Orthopractic motor neuroprosthetics**, which express volitions or reflex instructions that are naturally expressed by the hostmind and do so using the same modality and natural organic motor organs as are typically used by the hostmind.
- **Xenopractic motor neuroprosthetics**, which express a volition or reflex instruction through a modality that has been newly fashioned, made possible, or unlocked by the neuroprosthetic device and which is not one of the motor modalities naturally present in and used by the hostmind.
- **Xenergetic motor neuroprosthetics**, which express volitions or reflex instructions using a kind of motor organ (and resulting kind of motor action) that is not typically available to the hostmind's natural motor organs. Note that such devices may, however, use one of the hostmind's natural motor modalities, but in a way that is expressed using a nonstandard motor organ or actuator. The development of such devices – along with that of xenoceptive, xenesthetic, xenopractic, and xenosomatic neuroprosthetic devices – is a branch of **xenocybernetics**, which considers neuroprosthetic devices that grant their host or operator sensory, cognitive, or motor capacities or experiences that are alien to natural, unmodified human beings.<sup>30</sup>
- **Allopractic motor neuroprosthetics**, which express through one motor modality a volition or reflex instruction that is normally expressed through another modality (or not expressed by the hostmind at all).
- **Endopractic motor neuroprosthetics**, which express a volition or reflex action that normally is expressed externally to the host's body using motor modalities that relate to phenomena occurring within the host's body. For example, such a device might remap volitions that typically initiate and control oral speech or physical motion and use them to instead control a mechanism that regulates the release of hormones into the host's bloodstream.
- **Exopractic motor neuroprosthetics**, which express a volition or reflex action that normally is expressed internally to the host's body using motor modalities that relate to phenomena occurring externally to the

---

<sup>30</sup> See Gladden, "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences" (2015).

host's body. For example, such a device might remap volitions that normally control breathing, attention, or inner speech and instead use them to control an external robotic arm.



## Bibliography

- Abrams, Jerold J. "Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault." *Human Studies* 27, no. 3 (September 1, 2004): 241-58. doi:10.1023/B:HUMA.0000042130.79208.c6.
- Al-Hudhud, Ghada. "On Swarming Medical Nanorobots." *International Journal of Bio-Science & Bio-Technology* 4, no. 1 (March 2012): 75-90.
- Ameen, Moshaddique Al, Jingwei Liu, and Kyungsup Kwak. "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications." *Journal of Medical Systems* 36, no. 1 (March 12, 2010): 93-101. doi:10.1007/s10916-010-9449-4.
- Ankarali, Z.E., Q.H. Abbasi, A.F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan. "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security." In *2014 EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)*, 246-49, 2014. doi:10.1109/MOBIHEALTH.2014.7015957.
- Ansari, Sohail, K. Chaudhri, and K. Al Moutaery. "Vagus Nerve Stimulation: Indications and Limitations." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 281-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.
- Armando, Alessandro, Gabriele Costa, Alessio Merlo, and Luca Verderame. "Formal Modeling and Automatic Enforcement of Bring Your Own Device Policies." *International Journal of Information Security*, (August 10, 2014): 1-18. doi:10.1007/s10207-014-0252-y.
- Ayaz, Hasan, Patricia A. Shewokis, Scott Bunce, Maria Schultheis, and Banu Onaral. "Assessment of Cognitive Neural Correlates for a Functional Near Infrared-Based Brain Computer Interface System." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorow, Ivy V. Estabrooke, and Marc Grootjen, 699-708. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.
- Baars, Bernard J. *In the Theater of Consciousness*. New York, NY: Oxford University Press, 1997.

- Baddeley, Alan. "The episodic buffer: a new component of working memory?" *Trends in cognitive sciences* 4, no. 11 (2000): 417-423.
- Baudrillard, Jean. *Simulacra and Simulation*. Ann Arbor: University of Michigan Press, 1994.
- Berg, Bibi van den. "Pieces of Me: On Identity and Information and Communications Technology Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 159-73. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Bergamasco, S., M. Bon, and P. Inchingolo. "Medical data protection with a new generation of hardware authentication tokens." In *IFMBE Proceedings MEDICON 2001*, edited by R. Magjarevic, S. Tonkovic, V. Bilas, and I. Lackovic, 82-85. IFMBE, 2001.
- Birbaumer, Niels, and Klaus Haagen. "Restoration of Movement and Thought from Neuroelectric and Metabolic Brain Activity: Brain-Computer Interfaces (BCIs)." In *Intelligent Computing Everywhere*, edited by Dr Alfons J. Schuster, 129-52. Springer London, 2007.
- Birnbacher, Dieter. "Posthumanity, Transhumanism and Human Nature." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 95-106. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.
- Borkar, Shekhar. "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation." *Micro, IEEE* 25, no. 6 (2005): 10-16.
- Borton, D. A., Y.-K. Song, W. R. Patterson, C. W. Bull, S. Park, F. Laiwalla, J. P. Donoghue, and A. V. Nurmikko. "Implantable Wireless Cortical Recording Device for Primates." In *World Congress on Medical Physics and Biomedical Engineering, September 7-12, 2009, Munich, Germany*, edited by Olaf Dössel and Wolfgang C. Schlegel, 384-87. IFMBE Proceedings 25/9. Springer Berlin Heidelberg, 2009.
- Bostrom, Nick. "Why I Want to Be a Posthuman When I Grow Up." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 107-36. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.
- Bowman, Diana M., Mark N. Gasson, and Eleni Kosta. "The Societal Reality of That Which Was Once Science Fiction." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 175-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Braddon-Mitchell, David, and John Fitzpatrick. "Explanation and the Language of Thought." *Synthese* 83, no. 1 (April 1, 1990): 3-29. doi:10.1007/BF00413686.

- Bradshaw, Jeffrey M., Paul Feltovich, Matthew Johnson, Maggie Breedy, Larry Bunch, Tom Eskridge, Hyuckchul Jung, James Lott, Andrzej Uszok, and Jurriaan van Diggelen. "From Tools to Teammates: Joint Activity in Human-Agent-Robot Teams." In *Human Centered Design*, edited by Masaaki Kurosu, 935-44. Lecture Notes in Computer Science 5619. Springer Berlin Heidelberg, 2009.
- Brey, Philip. "Ethical Aspects of Information Security and Privacy." In *Security, Privacy, and Trust in Modern Data Management*, edited by Milan Petković and Willem Jonker, 21-36. Data-Centric Systems and Applications. Springer Berlin Heidelberg, 2007.
- Brunner, Peter, and Gerwin Schalk. "Brain-Computer Interaction." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorow, Ivy V. Estabrooke, and Marc Grootjen, 719-23. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.
- Buller, Tom. "Neurotechnology, Invasiveness and the Extended Mind." *Neuroethics* 6, no. 3 (August 18, 2011): 593-605. doi:10.1007/s12152-011-9133-5.
- Calverley, D.J. "Imagining a non-biological machine as a legal person." *AI & SOCIETY* 22, no. 4 (2008): 523-37.
- Campbell, Courtney S., James F. Keenan, David R. Loy, Kathleen Matthews, Terry Winograd, and Laurie Zoloth. "The Machine in the Body: Ethical and Religious Issues in the Bodily Incorporation of Mechanical Devices." In *Altering Nature*, edited by B. Andrew Lustig, Baruch A. Brody, and Gerald P. McKenny, 199-257. Philosophy and Medicine 98. Springer Netherlands, 2008.
- Cavallari, Maurizio. "Organisational Constraints on Information Systems Security." In *Emerging Themes in Information Systems and Organization Studies*, edited by Andrea Carugati and Cecilia Rossignoli, 193-207. Physica-Verlag HD, 2011.
- Cervera-Paz, Francisco Javier, and M. J. Manrique. "Auditory Brainstem Implants: Past, Present and Future Prospects." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 437-42. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.
- Chadwick, Ruth. "Therapy, Enhancement and Improvement." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 25-37. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.
- Chaudhry, Peggy E., Sohail S. Chaudhry, Ronald Reese, and Darryl S. Jones. "Enterprise Information Systems Security: A Conceptual Framework." In *Re-Conceptualizing Enterprise Information Systems*, edited by Charles Møller

- and Sohail Chaudhry, 118-28. *Lecture Notes in Business Information Processing* 105. Springer Berlin Heidelberg, 2012.
- Cho, Kwantae, and Dong Hoon Lee. "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks." In *Information Security Applications*, edited by Souhwan Jung and Moti Yung, 203-18. *Lecture Notes in Computer Science* 7115. Springer Berlin Heidelberg, 2012.
- Church, George M., Yuan Gao, and Sriram Kosuri. "Next-generation digital information storage in DNA." *Science* 337, no. 6102 (2012): 1628.
- Clark, Andy. "Systematicity, Structured Representations and Cognitive Architecture: A Reply to Fodor and Pylyshyn." In *Connectionism and the Philosophy of Mind*, edited by Terence Horgan and John Tienson, 198-218. *Studies in Cognitive Systems* 9. Springer Netherlands, 1991.
- Clark, S.S., and K. Fu, "Recent Results in Computer Security for Medical Devices," in *Wireless Mobile Communication and Healthcare*, edited by K.S. Nikita, J.C. Lin, D.I. Fotiadis, and M.-T. Arredondo Waldmeyer, 111-18. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* 83. Springer Berlin Heidelberg, 2012.
- Claussen, Jens Christian, and Ulrich G. Hofmann. "Sleep, Neuroengineering and Dynamics." *Cognitive Neurodynamics* 6, no. 3 (May 27, 2012): 211-14. doi:10.1007/s11571-012-9204-2.
- Clowes, Robert W. "The Cognitive Integration of E-Memory." *Review of Philosophy and Psychology* 4, no. 1 (January 26, 2013): 107-33. doi:10.1007/s13164-013-0130-y.
- Coeckelbergh, M. "From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots." *Philosophy & Technology* 24, no. 3 (2011): 269-78.
- Coles-Kemp, Lizzie, and Maranthi Theoharidou. "Insider Threat and Information Security Management." In *Insider Threats in Cyber Security*, edited by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop, 45-71. *Advances in Information Security* 49. Springer US, 2010.
- Cory, Jr., Gerald A. "Language, Brain, and Neuron." In *Toward Consilience*, 193-205. Springer US, 2000.
- Cosgrove, G.R. (2004). "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation." Meeting of the President's Council on Bioethics. Washington, DC, June 24-25, 2004. <https://bioethicsarchive.georgetown.edu/pcbe/transcripts/june04/session6.html>. Accessed June 12, 2015.
- Dardick, Glenn. "Cyber Forensics Assurance." In *Proceedings of the 8th Australian Digital Forensics Conference*, 57-64. Research Online, 2010.

- Datteri, E. "Predicting the Long-Term Effects of Human-Robot Interaction: A Reflection on Responsibility in Medical Robotics." *Science and Engineering Ethics* 19, no. 1 (2013): 139-60.
- Delac, Kresimir, and Mislav Grgic. "A Survey of Biometric Recognition Methods." In *Proceedings of the 46th International Symposium on Electronics in Marine, ELMAR 2004*, 184-93. IEEE, 2004.
- Denning, Tamara, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, and William H. Maisel. "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 917-26. ACM, 2010.
- Denning, Tamara, Kevin Fu, and Tadayoshi Kohno. "Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security." 3<sup>rd</sup> USENIX Workshop on Hot Topics in Security (HotSec 2008). San Jose, CA, July 29, 2008.
- Denning, Tamara, Yoky Matsuoka, and Tadayoshi Kohno. "Neurosecurity: Security and Privacy for Neural Devices." *Neurosurgical Focus* 27, no. 1 (2009): E7. doi:10.3171/2009.4.FOCUS985.
- Donchin, Emanuel, and Yael Arbel. "P300 Based Brain Computer Interfaces: A Progress Report." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 724-31. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.
- Drongelen, Wim van, Hyong C. Lee, and Kurt E. Hecox. "Seizure Prediction in Epilepsy." In *Neural Engineering*, edited by Bin He, 389-419. Bioelectric Engineering. Springer US, 2005.
- Dudai, Yadin. "The Neurobiology of Consolidations, Or, How Stable Is the Engram?" *Annual Review of Psychology* 55 (2004): 51-86. doi:10.1146/annurev.psych.55.090902.142050.
- Durand, Dominique M., Warren M. Grill, and Robert Kirsch. "Electrical Stimulation of the Neuromuscular System." In *Neural Engineering*, edited by Bin He, 157-91. Bioelectric Engineering. Springer US, 2005.
- Dvorsky, George. "What may be the world's first cybernetic hate crime unfolds in French McDonald's." i09, July 17, 2012. <http://i09.com/5926587/what-may-be-the-worlds-first-cybernetic-hate-crime-unfolds-in-french-mcdonalds>. Accessed July 22, 2015.

- Edgar, Andrew. "The Hermeneutic Challenge of Genetic Engineering: Habermas and the Transhumanists." *Medicine, Health Care and Philosophy* 12, no. 2 (May 1, 2009): 157-67. doi:10.1007/s11019-009-9188-9.
- Edlinger, Günter, Cristiano Rizzo, and Christoph Guger. "Brain Computer Interface." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 1003-17. Springer Berlin Heidelberg, 2011. [http://link.springer.com/chapter/10.1007/978-3-540-74658-4\\_52](http://link.springer.com/chapter/10.1007/978-3-540-74658-4_52).
- Erlr, Alexandre. "Does Memory Modification Threaten Our Authenticity?" *Neuroethics* 4, no. 3 (November 2011): 235-49. doi:10.1007/s12152-010-9090-4.
- Fairclough, S.H. "Physiological Computing: Interfacing with the Human Nervous System." In *Sensing Emotions*, edited by J. Westerink, M. Krans, and M. Ouwerkerk, 1-20. Philips Research Book Series 12. Springer Netherlands, 2010.
- Fernandes, Diogo A. B., Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio. "Security Issues in Cloud Environments: A Survey." *International Journal of Information Security* 13, no. 2 (September 28, 2013): 113-70. doi:10.1007/s10207-013-0208-7.
- Fernandez-Lopez, Helena, José A. Afonso, J. H. Correia, and Ricardo Simoes. "The Need for Standardized Tests to Evaluate the Reliability of Data Transport in Wireless Medical Systems." In *Sensor Systems and Software*, edited by Francisco Martins, Luís Lopes, and Hervé Paulino, 137-45. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 102. Springer Berlin Heidelberg, 2012.
- Ferrando, Francesca. "Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations." *Existenz: An International Journal in Philosophy, Religion, Politics, and the Arts* 8, no. 2 (Fall 2013): 26-32.
- "FIPA Device Ontology Specification." Foundation for Intelligent Physical Agents (FIPA), May 10, 2002. <http://www.fipa.org/assets/XC00091D.pdf>. Accessed February 9, 2015.
- Fleischmann, Kenneth R. "Sociotechnical Interaction and Cyborg-Cyborg Interaction: Transforming the Scale and Convergence of HCI." *The Information Society* 25, no. 4 (2009): 227-35. doi:10.1080/01972240903028359.
- Flemisch, F., M. Heesen, T. Hesse, J. Kelsch, A. Schieben, and J. Beller. "Towards a Dynamic Balance between Humans and Automation: Authority, Ability, Responsibility and Control in Shared and Cooperative Control Situations." *Cognition, Technology & Work* 14, no. 1 (2012): 3-18. doi:10.1007/s10111-011-0191-6.

- Fountas, Kostas N., and J. R. Smith. "A Novel Closed-Loop Stimulation System in the Control of Focal, Medically Refractory Epilepsy." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 357-62. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.
- Fox, S. and L. Rainie. "The Web at 25 in the US: Part 1: How the Internet Has Woven Itself into American Life." Pew Research Center's Internet & American Life Project, February 27, 2014. <http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/>. Accessed July 24, 2015.
- Freudenthal, Eric, Ryan Spring, and Leonardo Estevez. "Practical techniques for limiting disclosure of RF-equipped medical devices." In *Engineering in Medicine and Biology Workshop, 2007 IEEE Dallas*, 82-85. IEEE, 2007.
- Friedenberg, Jay. *Artificial Psychology: The Quest for What It Means to Be Human*, Philadelphia: Psychology Press, 2011.
- Gärtner, Armin. "Communicating Medical Systems and Networks." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 1085-93. Springer Berlin Heidelberg, 2011.
- Gasson, M.N., Kosta, E., and Bowman, D.M. "Human ICT Implants: From Invasive to Pervasive." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 1-8. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Gasson, M.N. "Human ICT Implants: From Restorative Application to Human Enhancement." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 11-28. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Gasson, M.N. "ICT implants." In *The Future of Identity in the Information Society*, edited by S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, 287-95. Springer US, 2008.
- Gerhardt, Greg A., and Patrick A. Tresco. "Sensor Technology." In *Brain-Computer Interfaces*, 7-29. Springer Netherlands, 2008.
- Gladden, Matthew E. "Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values." *Ethics in Economic Life*. Uniwersytet Łódzki, Łódź, May 8, 2015.
- Gladden, Matthew E. "Cybershells, Shapeshifting, and Neuroprosthetics: Video Games as Tools for Posthuman 'Body Schema (Re)Engineering'." *Ogólnopolska Konferencja Naukowa Dyskursy Gier Wideo. Facta Ficta*, AGH, Kraków, June 6, 2015.

- Gladden, Matthew E. "A Fractal Measure for Comparing the Work Effort of Human and Artificial Agents Performing Management Functions." In *Position Papers of the 2014 Federated Conference on Computer Science and Information Systems*, edited by Maria Ganzha, Leszek Maciaszek, Marcin Paprzycki, 219-26. Annals of Computer Science and Information Systems 3. Polskie Towarzystwo Informatyczne, 2014.
- Gladden, Matthew E. "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.
- Gladden, Matthew E. "The Social Robot as 'Charismatic Leader': A Phenomenology of Human Submission to Nonhuman Power." In *Sociable Robots and the Future of Social Relations: Proceedings of Robo-Philosophy 2014*, edited by Johanna Seibt, Raul Hakli, and Marco Nørskov, 329-39. Frontiers in Artificial Intelligence and Applications 273. IOS Press, 2014.
- Gladden, Matthew E. "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences." His Master's Voice: Utopias and Dystopias in Audiovisual Culture. Facta Ficta, Jagiellonian University, Kraków, March 24, 2015.
- Gladden, Matthew E. "'Upgrading' the Human Entity: Cyberization as a Path to Posthuman Utopia or Digital Annihilation?" Arkana Fantastyki lecture cycle. Centrum Informacji Naukowej i Biblioteka Akademicka (CINiBA), Katowice, May 27, 2015.
- Gordijn, Bert. "Converging NBIC Technologies for Improving Human Performance." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 225-35. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.
- Greenberg, Andy. "Cyborg Discrimination? Scientist Says McDonald's Staff Tried To Pull Off His Google-Glass-Like Eyepiece, Then Threw Him Out." *Forbes*, July 17, 2012. <http://www.forbes.com/sites/andygreenberg/2012/07/17/cyborg-discrimination-scientist-says-mcdonalds-staff-tried-to-pull-off-his-google-glass-like-eyepiece-then-threw-him-out/>. Accessed July 22, 2015.
- Grodzinsky, F.S., K.W. Miller, and M.J. Wolf. "Developing Artificial Agents Worthy of Trust: 'Would You Buy a Used Car from This Artificial Agent?'" *Ethics and Information Technology* 13, no. 1 (2011): 17-27.
- Grottke, M., H. Sun, R. M. Fricks, and K. S. Trivedi. "Ten fallacies of availability and reliability analysis." In *Service Availability*, 187-206. Lecture Notes in Computer Science 5017. Springer Berlin Heidelberg, 2008. [http://dx.doi.org/10.1007/978-3-540-68129-8\\_15](http://dx.doi.org/10.1007/978-3-540-68129-8_15).



- Gunkel, David, and Debra Hawhee. "Virtual Alterity and the Reformatting of Ethics." *Journal of Mass Media Ethics* 18, no. 3-4 (2003): 173-93. doi:10.1080/08900523.2003.9679663.
- Gunther, N. J. "Time—the zeroth performance metric." In *Analyzing Computer System Performance with Perl::PDQ*, 3-46. Berlin: Springer, 2005. [http://dx.doi.org/10.1007/978-3-540-26860-4\\_1](http://dx.doi.org/10.1007/978-3-540-26860-4_1).
- Halperin, Daniel, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses." In *IEEE Symposium on Security and Privacy*, 2008. *SP* 2008, 129-142. IEEE, 2008.
- Halperin, Daniel, Tadayoshi Kohno, Thomas S. Heydt-Benjamin, Kevin Fu, and William H. Maisel. "Security and privacy for implantable medical devices." *Pervasive Computing, IEEE* 7, no. 1 (2008): 30-39.
- Han, J.-H., S.A. Kushner, A.P. Yiu, H.-W. Hsiang, T. Buch, A. Waisman, B. Bontemp, R.L. Neve, P.W. Frankland, and S.A. Josselyn. "Selective Erasure of a Fear Memory." *Science* 323, no. 5920 (2009): 1492-96.
- Hansen, Jeremy A., and Nicole M. Hansen. "A Taxonomy of Vulnerabilities in Implantable Medical Devices." In *Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-Care Systems*, 13-20. ACM, 2010.
- Hanson, R. (1994). "If uploads come first: The crack of a future dawn." *Extropy* 6, no. 2 (1994), 10-15.
- Harrison, Ian. "IEC80001 and Future Ramifications for Health Systems Not Currently Classified as Medical Devices." In *Making Systems Safer*, edited by Chris Dale and Tom Anderson, 149-71. Springer London, 2010.
- Hatfield, B., A. Haufner, and J. Contreras-Vidal. "Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 810-17. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.
- Hei, Xiali, and Xiaojiang Du. "Biometric-based two-level secure access control for implantable medical devices during emergencies." In *INFOCOM, 2011 Proceedings IEEE*, 346-350. IEEE, 2011.
- Heersmink, Richard. "Embodied Tools, Cognitive Tools and Brain-Computer Interfaces." *Neuroethics* 6, no. 1 (September 1, 2011): 207-19. doi:10.1007/s12152-011-9136-2.

- Hellström, T. "On the Moral Responsibility of Military Robots," *Ethics and Information Technology* 15, no. 2 (2013): 99-107.
- Hern, Alex. "Hacker fakes German minister's fingerprints using photos of her hands." *The Guardian*, December 30, 2014. <http://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands>. Accessed July 24, 2015.
- Hildebrandt, Mireille, and Bernhard Anrig. "Ethical Implications of ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 135-58. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Hoffmann, Klaus-Peter, and Silvestro Micera. "Introduction to Neuroprosthetics." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 785-800. Springer Berlin Heidelberg, 2011.
- Humphreys, L., J. M. Ferrández, and E. Fernández. "Long Term Modulation and Control of Neuronal Firing in Excitable Tissue Using Optogenetics." In *Foundations on Natural and Artificial Computation*, edited by José Manuel Ferrández, José Ramón Álvarez Sánchez, Félix de la Paz, and F. Javier Toledo, 266-73. Lecture Notes in Computer Science 6686. Springer Berlin Heidelberg, 2011.
- Illes, Judy. *Neuroethics: Defining the Issues in Theory, Practice, and Policy*. Oxford University Press, 2006.
- Josselyn, Sheena A. "Continuing the Search for the Engram: Examining the Mechanism of Fear Memories." *Journal of Psychiatry & Neuroscience: JPN* 35, no. 4 (July 2010): 221-28. doi:10.1503/jpn.100015.
- Katz, Gregory. "The Hypothesis of a Genetic Protolanguage: An Epistemological Investigation." *Biosemiotics* 1, no. 1 (February 8, 2008): 57-73. doi:10.1007/s12304-008-9005-5.
- Kirkpatrick, K. "Legal Issues with Robots." *Communications of the ACM* 56, no. 11 (2013): 17-19.
- KleinOowski, A., Ethan H. Cannon, Phil Oldiges, and Larry Wissel. "Circuit design and modeling for soft errors." *IBM Journal of Research and Development* 52, no. 3 (2008): 255-63.
- Kłoda-Staniecko, Bartosz. "Ja, Cyborg. Trzy porządki, jeden byt. Podmiot jako fuzja biologii, kultury i technologii" ("I, Cyborg. Three Orders, One Being. Subject as a Fusion of Nature, Culture and Technology"). In *Człowiek w relacji do zwierząt, roślin i maszyn w kulturze: Tom I: Aspekt posthumanistyczny i transhumanistyczny*, edited by Justyna Tymienieckiej-Suchanek. Uniwersytet Śląski, 2015.

- Koch, K. P. "Neural Prostheses and Biomedical Microsystems in Neurological Rehabilitation." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 427-34. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.
- Koebler, Jason. "FCC Cracks Down on Cell Phone 'Jammers': The FCC says illegal devices that block cell phone signals could pose security risk." U.S. News & World Report, October 17, 2012. <http://www.usnews.com/news/articles/2012/10/17/fcc-cracks-down-on-cell-phone-jammers>. Accessed July 22, 2015.
- Koene, Randal A. "Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation." In *Singularity Hypotheses*, edited by Amnon H. Eden, James H. Moor, Johnny H. Søraker, and Eric Steinhart, 241-67. The Frontiers Collection. Springer Berlin Heidelberg, 2012.
- Kolkowska, Ella, and Gurpreet Dhillon. "Organizational Power and Information Security Rule Compliance." In *Future Challenges in Security and Privacy for Academia and Industry*, edited by Jan Camenisch, Simone Fischer-Hübner, Yuko Murayama, Armand Portmann, and Carlos Rieder, 185-96. IFIP Advances in Information and Communication Technology 354. Springer Berlin Heidelberg, 2011.
- Koops, B.-J., and R. Leenes (2012). "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 113-34. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Kosta, E., and D.M. Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 97-112. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Kourany, J.A. (2013). "Human enhancement: Making the debate more Productive." *Erkenntnis* 79, no. 5 (2013): 981-98.
- Kowalewska, Agata. "Symbionts and Parasites – Digital Ecosystems." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.
- Kraemer, Felicitas. "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation." *Neuroethics* 6, no. 3 (May 12, 2011): 483-97. doi:10.1007/s12152-011-9115-7.

- Kuflik, A. "Computers in Control: Rational Transfer of Authority or Irresponsible Abdication of Autonomy?" *Ethics and Information Technology* 1, no. 3 (1999): 173-84.
- Lebedev, M., "Brain-Machine Interfaces: An Overview," *Translational Neuroscience* 5, no. 1 (March 28, 2014): 99-110.
- Leder, Felix, Tillmann Werner, and Peter Martini. "Proactive Botnet Countermeasures: An Offensive Approach." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 211-25. Cryptology and Information Security Series. IOS Press, 2009. doi:10.3233/978-1-60750-060-5-211.
- Lee, Giljae, Andréa Matsunaga, Salvador Dura-Bernal, Wenjie Zhang, William W. Lytton, Joseph T. Francis, and José AB Fortes. "Towards Real-Time Communication between in Vivo Neurophysiological Data Sources and Simulator-Based Brain Biomimetic Models." *Journal of Computational Surgery* 3, no. 1 (November 11, 2014): 1-23. doi:10.1186/s40244-014-0012-3.
- Li, S., F. Hu, and G. Li, "Advances and Challenges in Body Area Network." In *Applied Informatics and Communication*, edited by J. Zhan, 58-65. Communications in Computer and Information Science 22. Springer Berlin Heidelberg, 2011.
- Linsenmeier, Robert A. "Retinal Bioengineering." In *Neural Engineering*, edited by Bin He, 421-84. Bioelectric Engineering. Springer US, 2005.
- Lloyd, David. "Biological Time Is Fractal: Early Events Reverberate over a Life Time." *Journal of Biosciences* 33, no. 1 (March 1, 2008): 9-19. doi:10.1007/s12038-008-0017-8.
- Longuet-Higgins, H.C. "Holographic Model of Temporal Recall." *Nature* 217, no. 5123 (1968): 104. doi:10.1038/217104a0.
- Lorence, Daniel, Anusha Sivaramakrishnan, and Michael Richards. "Transaction-Neutral Implanted Data Collection Interface as EMR Driver: A Model for Emerging Distributed Medical Technologies." *Journal of Medical Systems* 34, no. 4 (March 20, 2009): 609-17. doi:10.1007/s10916-009-9274-9.
- Lucivero, Federica, and Guglielmo Tamburrini. "Ethical Monitoring of Brain-Machine Interfaces." *AI & SOCIETY* 22, no. 3 (August 3, 2007): 449-60. doi:10.1007/s00146-007-0146-x.
- Ma, Ting, Ying-Ying Gu, and Yuan-Ting Zhang. "Circuit Models for Neural Information Processing." In *Neural Engineering*, edited by Bin He, 333-65. Bioelectric Engineering. Springer US, 2005.
- MacVittie, Kevin, Jan Halánek, Lenka Halámková, Mark Southcott, William D. Jemison, Robert Lobel, and Evgeny Katz. "From 'cyborg' lobsters to a pacemaker powered by implantable biofuel cells." *Energy & Environmental Science* 6, no. 1 (2013): 81-86.

- Maj, Krzysztof. "Rational Technotopia vs. Corporational Dystopia in 'Deus Ex: Human Revolution' Gameworld." *His Master's Voice: Utopias and Dystopias in Audiovisual Culture. Facta Ficta*, Jagiellonian University, Kraków, March 24, 2015.
- Mak, Stephen. "Ethical Values for E-Society: Information, Security and Privacy." In *Ethics and Policy of Biometrics*, edited by Ajay Kumar and David Zhang, 96-101. *Lecture Notes in Computer Science 6005*. Springer Berlin Heidelberg, 2010.
- Masani, Kei, and Milos R. Popovic. "Functional Electrical Stimulation in Rehabilitation and Neurorehabilitation." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 877-96. Springer Berlin Heidelberg, 2011.
- McCormick, Michael. "Data Theft: A Prototypical Insider Threat." In *Insider Attack and Cyber Security*, edited by Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith, and Sara Sinclair, 53-68. *Advances in Information Security 39*. Springer US, 2008.
- McCullagh, P., G. Lightbody, J. Zygierevicz, and W.G. Kernohan, "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology." *Neuroethics* 7, no. 2 (July 28, 2013): 109-22.
- McGee, E.M., "Bioelectronics and Implanted Devices." In *Medical Enhancement and Posthumanity*, edited by B. Gordijn and R. Chadwick, 207-24. *The International Library of Ethics, Law and Technology 2*. Springer Netherlands, 2008.
- McGrath, Michael J., and Cliodhna Ní Scanaill. "Regulations and Standards: Considerations for Sensor Technologies." In *Sensor Technologies*, 115-35. Apress, 2013.
- Meloy, Stuart. "Neurally Augmented Sexual Function." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 359-63. *Acta Neurochirurgica Supplements 97/1*. Springer Vienna, 2007.
- Merkel, R., G. Boer, J. Fegert, T. Galert, D. Hartmann, B. Nuttin, and S. Rosahl, "Central Neural Prostheses." In *Intervening in the Brain: Changing Psyche and Society*, 117-60. *Ethics of Science and Technology Assessment 29*. Springer Berlin Heidelberg, 2007.
- Miah, Andy. "A Critical History of Posthumanism." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 71-94. *The International Library of Ethics, Law and Technology 2*. Springer Netherlands, 2008.

- Miller, Kai J., and Jeffrey G. Ojemann. "A Simple, Spectral-Change Based, Electrographic Brain-Computer Interface." In *Brain-Computer Interfaces*, edited by Bernhard Graimann, Gert Pfurtscheller, and Brendan Allison, 241-58. The Frontiers Collection. Springer Berlin Heidelberg, 2009.
- Mitcheson, Paul D. "Energy harvesting for human wearable and implantable bio-sensors." In *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, 3432-3436. IEEE, 2010.
- Mizraji, Eduardo, Andrés Pomi, and Juan C. Valle-Lisboa. "Dynamic Searching in the Brain." *Cognitive Neurodynamics* 3, no. 4 (June 3, 2009): 401-14. doi:10.1007/s11571-009-9084-2.
- Moravec, Hans. *Mind Children: The Future of Robot and Human Intelligence*. Cambridge: Harvard University Press, 1990.
- Moxon, Karen A. "Neurorobotics." In *Neural Engineering*, edited by Bin He, 123-55. Bioelectric Engineering. Springer US, 2005.
- Negoescu, R. "Conscience and Consciousness in Biomedical Engineering Science and Practice." In *International Conference on Advancements of Medicine and Health Care through Technology*, edited by Simona Vlad, Radu V. Ciupa, and Anca I. Nicu, 209-14. IFMBE Proceedings 26. Springer Berlin Heidelberg, 2009.
- Neuper, Christa, and Gert Pfurtscheller. "Neurofeedback Training for BCI Control." In *Brain-Computer Interfaces*, edited by Bernhard Graimann, Gert Pfurtscheller, and Brendan Allison, 65-78. The Frontiers Collection. Springer Berlin Heidelberg, 2009.
- NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security*. Edited by Gary Stoneburner. Gaithersburg, Maryland: National Institute of Standards & Technology, 2001.
- NIST Special Publication 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Joint Task Force Transformation Initiative. Gaithersburg, Maryland: National Institute of Standards & Technology, 2010.
- NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative. Gaithersburg, Maryland: National Institute of Standards & Technology, 2013.
- NIST Special Publication 800-70, Revision 2: National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*. Edited by Stephen D. Quinn, Murugiah P. Souppaya, Melanie Cook, and Karen A. Scarfone. Gaithersburg, Maryland: National Institute of Standards & Technology, 2011.

- NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers*. Edited by P. Bowen, J. Hash, and M. Wilson. Gaithersburg, Maryland: National Institute of Standards & Technology, 2006.
- Overman, Stephenie. "Jamming Employee Phones Illegal." Society for Human Resource Management, May 9, 2014. <http://www.shrm.org/hrdisciplines/technology/articles/pages/cell-phone-jamming.aspx>. Accessed July 22, 2015.
- Pająk, Robert. Email correspondence with the author, May 3, 2015.
- Panoulas, Konstantinos J., Leontios J. Hadjileontiadis, and Stavros M. Panas. "Brain-Computer Interface (BCI): Types, Processing Perspectives and Applications." In *Multimedia Services in Intelligent Environments*, edited by George A. Tsihrintzis and Lakhmi C. Jain, 299-321. Smart Innovation, Systems and Technologies 3. Springer Berlin Heidelberg, 2010.
- Park, M.C., M.A. Goldman, T.W. Belknap, and G.M. Friehs, "The Future of Neural Interface Technology." In *Textbook of Stereotactic and Functional Neurosurgery*, edited by A.M. Lozano, P.L. Gildenberg, and R.R. Tasker, 3185-3200. Heidelberg/Berlin: Springer, 2009.
- Parker, Donn "Our Excessively Simplistic Information Security Model and How to Fix It." *ISSA Journal* (July 2010): 12-21.
- Parker, Donn B. "Toward a New Framework for Information Security." In *The Computer Security Handbook*, 4th Ed., edited by Seymour Bosworth and M. E. Kabay. John Wiley & Sons, 2002.
- Passeraub, Ph A., and N. V. Thakor. "Interfacing Neural Tissue with Microsystems." In *Neural Engineering*, edited by Bin He, 49-83. Bioelectric Engineering. Springer US, 2005.
- Patil, P.G., and D.A. Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices." In *Neurotherapeutics* 5, no. 1 (January 1, 2008): 137-46.
- Pearce, David, "The Bointelligence Explosion." In *Singularity Hypotheses*, edited by A.H. Eden, J.H. Moor, J.H. Søraker, and E. Steinhart, 199-238. The Frontiers Collection. Berlin/Heidelberg: Springer, 2012.
- Polikov, Vadim S., Patrick A. Tresco, and William M. Reichert. "Response of brain tissue to chronically implanted neural electrodes." *Journal of Neuroscience Methods* 148, no. 1 (2005): 1-18.
- Prestes, E., J.L. Carbonera, S. Rama Fiorini, V.A.M. Jorge, M. Abel, R. Madhavan, A. Locoro, et al., "Towards a Core Ontology for Robotics and Automation." *Robotics and Autonomous Systems*, Ubiquitous Robotics 61, no. 11 (November 2013): 1193-1204.

- Pribram, K. H. "Prolegomenon for a Holonomic Brain Theory." In *Synergetics of Cognition*, edited by Hermann Haken and Michael Stadler, 150-84. Springer Series in Synergetics 45. Springer Berlin Heidelberg, 1990.
- Pribram, K.H., and S.D. Meade. "Conscious Awareness: Processing in the Synaptodendritic Web - The Correlation of Neuron Density with Brain Size." *New Ideas in Psychology* 17, no. 3 (December 1, 1999): 205-14. doi:10.1016/S0732-118X(99)00024-0.
- Principe, José C., and Dennis J. McFarland. "BMI/BCI Modeling and Signal Processing." In *Brain-Computer Interfaces*, 47-64. Springer Netherlands, 2008.
- Proudfoot, Diane. "Software Immortals: Science or Faith?" In *Singularity Hypotheses*, edited by Amnon H. Eden, James H. Moor, Johnny H. Søraker, and Eric Steinhart, 367-92. The Frontiers Collection. Springer Berlin Heidelberg, 2012.
- Qureshi, Mohmad Kashif. "Liveness detection of biometric traits." *International Journal of Information Technology and Knowledge Management* 4 (2011): 293-95.
- Rahimi, Ali, Ben Recht, Jason Taylor, and Noah Vawter. "On the effectiveness of aluminium foil helmets: An empirical study." MIT, February 17, 2005. <http://web.archive.org/web/20100708230258/http://peo-plpe.csail.mit.edu/rahimi/helmet/>. Accessed July 26, 2015.
- Ramirez, S., X. Liu, P.-A. Lin, J. Suh, M. Pignatelli, R.L. Redondo, T.J. Ryan, and S. Tonegawa. "Creating a False Memory in the Hippocampus." *Science* 341, no. 6144 (2013): 387-91.
- Rao, R.P.N., A. Stocco, M. Bryan, D. Sarma, T.M. Youngquist, J. Wu, and C.S. Prat. "A direct brain-to-brain interface in humans." *PLoS ONE* 9, no. 11 (2014).
- Rao, Umesh Hodeghatta, and Umesha Nayak. *The InfoSec Handbook*. New York: Apress, 2014.
- Rasmussen, Kasper Bonne, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. "Proximity-based access control for implantable medical devices." In *Proceedings of the 16th ACM conference on Computer and communications security*, 410-19. ACM, 2009.
- Reynolds, Dwight W., Christina M. Murray, and Robin E. Germany. "Device Therapy for Remote Patient Management." In *Electrical Diseases of the Heart*, edited by Ihor Gussak, Charles Antzelevitch, Arthur A. M. Wilde, Paul A. Friedman, Michael J. Ackerman, and Win-Kuang Shen, 809-25. Springer London, 2008.



- Robinett, W. "The consequences of fully understanding the brain." In *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*, edited by M.C. Roco and W.S. Bainbridge, 166-70. National Science Foundation, 2002.
- Roosendaal, Arnold. "Carrying Implants and Carrying Risks; Human ICT Implants and Liability." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 69-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Roosendaal, Arnold. "Implants and Human Rights, in Particular Bodily Integrity." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 81-96. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Rossebeø, J. E. Y., M. S. Lund, K. E. Husa, and A. Refsdal, "A conceptual model for service availability." In *Quality of Protection*, 107-18. Advances in Information Security 23. Springer US, 2006.
- Rotter, Pawel, Barbara Daskala, and Ramon Compañó. "Passive Human ICT Implants: Risks and Possible Solutions." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 55-62. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Rotter, Pawel, Barbara Daskala, Ramon Compañó, Bernhard Anrig, and Claude Fuhrer. "Potential Application Areas for RFID Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 29-39. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Rotter, Pawel, and Mark N. Gasson. "Implantable Medical Devices: Privacy and Security Concerns." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 63-66. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Rubin, Charles T. "What Is the Good of Transhumanism?" In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 137-56. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.
- Rutten, W. L. C., T. G. Ruardij, E. Marani, and B. H. Roelofsen. "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe." In *Operative Neuromodulation*, edited by Damianos E. Sakas and

- Brian A. Simpson, 547-54. *Acta Neurochirurgica Supplements* 97/2. Springer Vienna, 2007.
- Sakas, Damianos E., I. G. Panourias, and B. A. Simpson. "An Introduction to Neural Networks Surgery, a Field of Neuromodulation Which Is Based on Advances in Neural Networks Science and Digitised Brain Imaging." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 3-13. *Acta Neurochirurgica Supplements* 97/2. Springer Vienna, 2007.
- Sasse, Martina Angela, Sacha Brostoff, and Dirk Weirich. "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." *BT technology journal* 19, no. 3 (2001): 122-131.
- Sayrafian-Pour, K., W.-B. Yang, J. Hagedorn, J. Terrill, K. Yekeh Yazdandoost, and K. Hamaguchi. "Channel Models for Medical Implant Communication." *International Journal of Wireless Information Networks* 17, no. 3-4 (December 9, 2010): 105-12.
- Schechter, Stuart. "Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices." Microsoft Research, August 10, 2010. <http://research.microsoft.com:8082/apps/pubs/default.aspx?id=135291>. Accessed July 26, 2015.
- Schermer, Maartje. "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction." *NanoEthics* 3, no. 3 (December 1, 2009): 217-30. doi:10.1007/s11569-009-0076-9.
- Shih, J. "Project time in Silicon Valley." *Qualitative Sociology* 27, no. 2 (June 1, 2004): 223-45.
- Shoniregun, Charles A., Kudakwashe Dube, and Fredrick Mtenzi. "Introduction to E-Healthcare Information Security." In *Electronic Healthcare Information Security*, 1-27. *Advances in Information Security* 53. Springer US, 2010.
- Smolensky, Paul. "The Constituent Structure of Connectionist Mental States: A Reply to Fodor and Pylyshyn." In *Connectionism and the Philosophy of Mind*, edited by Terence Horgan and John Tienson, 281-308. *Studies in Cognitive Systems* 9. Springer Netherlands, 1991.
- Soussou, Walid V., and Theodore W. Berger. "Cognitive and Emotional Neuroprostheses." In *Brain-Computer Interfaces*, 109-23. Springer Netherlands, 2008.
- Spohrer, Jim, "NBICS (Nano-Bio-Info-Cogno-Socio) Convergence to Improve Human Performance: Opportunities and Challenges." In *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*, edited by M.C. Roco and W.S. Bainbridge, 101-17. Arlington, Virginia: National Science Foundation, 2002.

- Srinivasan, G. R. "Modeling the cosmic-ray-induced soft-error rate in integrated circuits: an overview." *IBM Journal of Research and Development* 40, no. 1 (1996): 77-89.
- Stahl, B. C. "Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency." *Ethics and Information Technology* 8, no. 4 (2006): 205-13.
- Stieglitz, Thomas. "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Bio-hybrid Systems." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 435-42. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.
- Szczepocka, Magdalena. "Konflikt sprzecznych utopii jako główny problem gry fabularnej 'Mag: Wstąpienie'." *Głos Pana: Utopie i dystopie w kulturze audio-wizualnej*. Facta Ficta, Jagiellonian University, Kraków, March 27, 2015.
- Tadeusiewicz, Ryszard, Pawel Rotter, and Mark N. Gasson. "Restoring Function: Application Exemplars of Medical ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 41-51. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.
- Taira, Takaomi, and T. Hori. "Diaphragm Pacing with a Spinal Cord Stimulator: Current State and Future Directions." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 289-92. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.
- Tamburrini, Guglielmo. "Brain to Computer Communication: Ethical Perspectives on Interaction Models." *Neuroethics* 2, no. 3 (March 11, 2009): 137-49. doi:10.1007/s12152-009-9040-1.
- Tarín, C., L. Traver, P. Martí, and N. Cardona. "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring." In *Wireless Technology*, edited by S. Powell and J.P. Shim, 177-201. Lecture Notes in Electrical Engineering 44. Springer US, 2009.
- Taylor, N. R., and J. G. Taylor. "The Neural Networks for Language in the Brain: Creating LAD." In *Computational Models for Neuroscience*, edited by Robert Hecht-Nielsen and Thomas McKenna, 245-65. Springer London, 2003.
- Taylor, Dawn M. "Functional Electrical Stimulation and Rehabilitation Applications of BCIs." In *Brain-Computer Interfaces*, 81-94. Springer Netherlands, 2008.

- Thanos, Solon, P. Heiduschka, and T. Stupp. "Implantable Visual Prostheses." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 465-72. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.
- Thonnard, Olivier, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, and Martin Lee. "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat." In *Research in Attacks, Intrusions, and Defenses*, edited by Davide Balzarotti, Salvatore J. Stolfo, and Marco Cova, 64-85. Lecture Notes in Computer Science 7462. Springer Berlin Heidelberg, 2012.
- Thorpe, Julie, Paul C. van Oorschot, and Anil Somayaji. "Pass-thoughts: authenticating with our minds." In *Proceedings of the 2005 Workshop on New Security Paradigms*, 45-56. ACM, 2005.
- Troyk, Philip R., and Stuart F. Cogan. "Sensory Neural Prostheses." In *Neural Engineering*, edited by Bin He, 1-48. Bioelectric Engineering. Springer US, 2005.
- Ullah, Sana, Henry Higgin, M. Arif Siddiqui, and Kyung Sup Kwak. "A Study of Implanted and Wearable Body Sensor Networks." In *Agent and Multi-Agent Systems: Technologies and Applications*, edited by Ngoc Thanh Nguyen, Geun Sik Jo, Robert J. Howlett, and Lakhmi C. Jain, 464-73. Lecture Notes in Computer Science 4953. Springer Berlin Heidelberg, 2008.
- U.S. Code, Title 44 (Public Printing and Documents), Subchapter III (Information Security), Section 3542 (Definitions), cited in *NIST Special Publication 800-37, Revision 1*.
- Voldjounaite, Elena, Satu-Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, and Heikki Ailisto. "Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices." In *Pervasive Computing*, edited by Kenneth P. Fishkin, Bernt Schiele, Paddy Nixon, and Aaron Quigley, 187-201. Lecture Notes in Computer Science 3968. Springer Berlin Heidelberg, 2006.
- Viola, M. V., and Aristides A. Patrinos. "A Neuroprosthesis for Restoring Sight." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 481-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.
- Warwick, K. "The cyborg revolution." *Nanoethics* 8 (2014): 263-73.
- Warwick, K., and M. Gasson, "Implantable Computing." In *Digital Human Modeling*, edited by Y. Cai, 1-16. Lecture Notes in Computer Science 4650. Berlin/Heidelberg: Springer, 2008.
- Weber, R. H., and Weber, R. "General Approaches for a Legal Framework." In *Internet of Things*, 23-40. Springer Berlin/Heidelberg, 2010.

- Weiland, James D., Wentai Liu, and Mark S. Humayun. "Retinal Prosthesis." *Annual Review of Biomedical Engineering* 7, no. 1 (2005): 361-401. doi:10.1146/annurev.bioeng.7.060804.100435.
- Weinberger, Sharon. "Mind Games." *The Washington Post*, January 14, 2007. [http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399_pf.html). Accessed July 26, 2015.
- Werkhoven, Peter. "Experience Machines: Capturing and Retrieving Personal Content." In *E-Content*, edited by Peter A. Bruck, Zeger Karssen, Andrea Buchholz, and Ansgar Zerfass, 183-202. Springer Berlin Heidelberg, 2005.
- Widge, A.S., C.T. Moritz, and Y. Matsuoka. "Direct Neural Control of Anatomically Correct Robotic Hands." In *Brain-Computer Interfaces*, edited by D.S. Tan and A. Nijholt, 105-19. Human-Computer Interaction Series. London: Springer, 2010.
- Wiener, Norbert. *Cybernetics: Or Control and Communication in the Animal and the Machine*, second edition. Cambridge, Massachusetts: The MIT Press, 1961 (Quid Pro ebook edition for Kindle, 2015).
- Wilkinson, Jeff, and Scott Hareland. "A cautionary tale of soft errors induced by SRAM packaging materials." *IEEE Transactions on Device and Materials Reliability* 5, no. 3 (2005): 428-433.
- Wiltshire, Travis J., Dustin C. Smith, and Joseph R. Keebler. "Cybernetic Teams: Towards the Implementation of Team Heuristics in HRI." In *Virtual Augmented and Mixed Reality. Designing and Developing Augmented and Virtual Environments*, edited by Randall Shumaker, 321-30. Lecture Notes in Computer Science 8021. Springer Berlin Heidelberg, 2013.
- Zamanian, Ali, and Cy Hardiman. "Electromagnetic radiation and human health: A review of sources and effects." *High Frequency Electronics* 4, no. 3 (2005): 16-26.
- Zarod, Marcin. "Constructing Hackers. Professional Biographies of Polish Hackers." *Digital Ecosystems*. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.
- Zebda, Abdelkader, S. Cosnier, J.-P. Alcaraz, M. Holzinger, A. Le Goff, C. Gondran, F. Boucher, F. Giroud, K. Gorgy, H. Lamraoui, and P. Cinquin. "Single glucose biofuel cells implanted in rats power electronic devices." *Scientific Reports* 3, article 1516 (2013). doi:10.1038/srep01516.
- Zhao, QiBin, LiQing Zhang, and Andrzej Cichocki. "EEG-Based Asynchronous BCI Control of a Car in 3D Virtual Reality Environments." *Chinese Science Bulletin* 54, no. 1 (January 11, 2009): 78-87. doi:10.1007/s11434-008-0547-3.

- Zheng, Guanglou, Gengfa Fang, Mehmet Orgun, and Rajan Shankaran. "A Non-key based security scheme supporting emergency treatment of wireless implants." In *2014 IEEE International Conference on Communications (ICC)*, 647-52. IEEE, 2014.
- Zheng, Guanglou, Gengfa Fang, Mehmet Orgun, Rajan Shankaran, and Eryk Dutkiewicz. "Securing wireless medical implants using an ECG-based secret data sharing scheme." In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, 373-77. IEEE, 2014.
- Zheng, Guanglou, Gengfa Fang, Rajan Shankaran, Mehmet Orgun, and Eryk Dutkiewicz. "An ECG-based secret data sharing scheme supporting emergency treatment of Implantable Medical Devices." In *2014 International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 624-28. IEEE, 2014.



## Index

- access agreements ..... 227
- access controls ..... 273
  - for output devices ..... 229
  - mandatory ..... 274
  - physical ..... 228
- access enforcement ..... 274
- account management ..... 273
- accreditation ..... 178, 221
- acoustic wayfaring ..... 314
- acquisition process ..... 211
- acquisition, system and services . 211
- active neuroprosthetics ..... 31
- actuator ..... 321
- adaptive identification and
  - authentication ..... 272
- additions ..... 25, 55
- address resolution service ..... 292
- adversaries ..... 49, 83
  - active ..... 49
  - coordinated ..... 49
  - passive ..... 49
  - types of ..... 49
- advisories, security ..... 249
- agency ..... 152, 165
- alarms ..... 228, 230
- alerts ..... 249
  - audible ..... 78
- allocation of resources ..... 211
- alloesthetic neuroprosthetics ..... 316
- allopractic motor neuroprosthetics ..... 324
- allow by exception ..... 286
- ALS ..... 24, 99
- alternate processing site ..... 235
- alternate storage site ..... 235
- alternative security mechanisms 237
- Alzheimer's disease ..... 25
- analysis
  - malicious code ..... 244
  - security impact ..... 237
- anomalies, communications traffic ..... 245
- anxiety disorders ..... 25
- application developers ..... 186
- application partitioning ..... 282
- artificial eye ..... 67
- asset monitoring and tracking... 234
- attack surface reviews ..... 214
- attacks
  - active ..... 50
  - passive ..... 50
  - resource depletion ..... 56
  - types of ..... 49
- atypical usage ..... 274
- audioceptive neuroprosthetics .. 309
- audioesthetic neuroprosthetics .. 312
- audit and accountability ..... 280
- audit events ..... 280
- audit processing failures ..... 281
- audit storage capacity ..... 280
- auditory cortex ..... 312, 314
- augmented reality ..... 23



- ul style="list-style-type: none; padding-left: 0;">
- authentication .....44
- authenticator feedback .....271
- authenticator management .....270
- authenticity ..... 16, 96, 135, 143
  - session .....292
- authorization .....44
- automated testing .....262
- automated training environments
  - .....261
- autonomy .....16, 96, 139, 142
- availability ..... 16, 39, 65, 133, 142
  - resource .....284
- awareness .....265
- backup ..... 41
  - information system .....236
- balance, sense of .....309, 313
- basal ganglia ..... 311, 314
- baseline configuration .....237
- behavior changes .....88
- belief-related neuroprosthetics...318
- benchmarks for corrective action
  - .....242
- bidirectional sensorimotor
  - neuroprosthetics .....26
- biocybernetic system architecture
  - .....210
- biocybernetics..... 17, 101, 306
- biological processes..... 120, 122, 159
  - autonomous regulation.....311
- biomedical and bioengineering
  - specifications .....210
- biomedical engineering ..... 100
- biometrics .....84, 271
- biomolecular computing ..22, 36, 90, 92
- bionanotechnology .....22, 90
- blackmail .....167
- bladder function .....24
- blood pressure .....86
- Bluetooth..... 121
- bodily organs .....309
- body area networks (BANs) ..... 19
- body schema.....199
- body sensor networks (BSNs) .....19
- boundary protection..... 285
- bracelets.....73
- brain stem..... 313
- brain-computer interfaces (BCIs)25, 29
- brain-machine interfaces (BMIs) 20
- breathing .....85, 323
- bulimia .....25
- central management.....210, 241
- cerebellum..... 311, 313, 314
- cerebral cortex .....311, 314
- cerebrum ..... 313
- certificate schemes ..... 71
- certification ..... 177, 221
- chain of custody .....281
- chemoreceptive neuroprosthetics
  - .....310
- chemoreceptors ..... 310
- chief information officer (CIO) ..192
- chronoception ..... 310
- chronoceptive neuroprosthetics 310
- chronoesthetic neuroprosthetics 313
- CIA Triad ..... 15, 39, 130
- classified information.....225
- cloaking device..... 77
- closed-circuit TV..... 44
- cochlear implants ..... 19, 23
- cochlear nerve ..... 312, 314
- cognitive security framework ..16, 129
- cognitive and noetic security plans
  - .....210
- cognitive neuroprosthetics ... 26, 316
- collaborative computing devices 291
- component authenticity..... 220
- concealment and misdirection.. 296
- concealment of communications
  - .....289
- concurrent session control ..... 278
- confidentiality .....16, 39, 130, 143

- transmission .....289
- configuration change control..... 237
- configuration management .178, 213, 237
- conscience ..... 98, 151, 320
- consciousness ..... 96, 151, 153, 317
- consciousness-related
  - neuroprosthetics .....319
- container-based encryption .....279
- contingency plan testing ..... 235
- contingency planning .....234
- contingency training ..... 235
- controlled release ..... 275
- controls .....40
  - administrative .....40
  - logical ..... 41
  - management.....205
  - operational ..... 223
  - physical .....40
  - technical .....267
- corporate espionage .....167
- costs .....111, 174
- countermeasures
  - corrective .....71
  - detective .....71
  - protective.....71
- covert channel analysis.....297
- covert channels.....284
- creativity.....149
- criticality analysis.....217
- cryptographic keys ..... 73
  - establishment .....290
- cryptographic protection.....289
- customization ..... 111
- customized development of critical
  - components .....221
- cyberization .....94
- cybernetics ..... 101
- cyberwarfare ..... 34
- cyborgs .....20
- data mining protection .....280
- deep brain stimulation ..... 19, 97
- defibrillators ..... 19
- denial of service attacks.....56
- denial of service protection .....284
- deny by default..... 286
- dependencies..... 153
- design
  - conceptually simple ..... 219
- designers..... 109, 181
  - body .....199
- detection potential ..... 301
- detonation chambers..... 304
- developer configuration
  - management..... 213
- developer security architecture and
  - design..... 219
- developer security testing and
  - evaluation ..... 213
- development process..... 218
- device attestation..... 269
- device-host system ..... 80
- diagnosis ..... 28
- digestion .....323
- directives, security ..... 249
- discovery, device .....112, 288
- disposal ..... 180, 181
- distinguishability .....16, 138, 143
- distributed processing and storage
  - ..... 299
- DNA .....22, 85, 89, 91
- documentation, information
  - system ..... 212
- domain authentication..... 276
- drowsiness ..... 310
- dual authorization ..... 274
- dynamic information flow control
  - .....275
- dynamic reconfiguration..... 262
- ear geometry..... 84
- early adopters..... 34
- eavesdropping .....51, 52, 53, 54
- ECG ..... 87
- echoesthetic neuroprosthetics ... 314
- echolocation ..... 314
- EEG.....25
- electric charge ..... 308
- electrocorticography (ECoG).....25
- electroesthetic neuroprosthetics 314
- electromagnetic interference..... 300

- electromagnetic radiation .....308
- electroreceptive neuroprosthetics
  - .....308
- electroreceptors.....308
- embedded data types .....275
- embodied embedded organism,
  - host as.....17, 146, 155
- emergency access .....69
- emergency accounts.....273
- emergency power .....232
- emergency shutoff.....231
- emotional neuroprosthetics 150, 318
- endoesthetic neuroprosthetics ...316
- endopractic motor
  - neuroprosthetics .....324
- engineers
  - body schema.....199
  - neuromnemonic .....200
  - sensory .....201
- engrams.....149, 154
- environmental protection .....227
- environments, protected .....251
- epersonality-related
  - neuroprosthetics .....318
- epilepsy.....25
- episodic buffer .....319
- equilibrioception .....309
- equilibrioceptive neuroprosthetics
  - .....309
- equilibrioesthetic neuroprosthetics
  - .....313
- error handling.....253
- ethics .....100
- executable code .....251
- executable programs
  - non-modifiable .....298
- exfiltration
  - covert .....247
  - unauthorized.....287
- exoesthetic neuroprosthetics .....316
- exograms .....156
- exopractic motor neuroprosthetics
  - .....324
- external information systems ....212, 279
- extortion .....167
- eye, artificial .....67
- facial geometry.....84
- fail in known state .....292
- fail open .....77
- fail secure.....288
- failover capability.....255
- fail-safe.....259
- fingerprints.....84, 86
- fire protection .....233
- firmware.....249, 251
- flaw remediation .....241
- fMRI .....21
- formal policy model.....219
- functional electrical stimulation (FES).....25
- functional near infrared spectroscopy (fNIR).....25
- gait.....85, 88
- gamma rays .....308
- gateway, external .....78
- Global Workspace Theory .....259
- glucose level, blood .....85
- guards .....228
- gustatoesthetic neuroprosthetics312
- gustatory cortex .....312
- gustatory neuroprosthetics.....310
- habit-related neuroprosthetics..320
- hair cells.....309
- hand geometry .....84
- haptic motor neuroprosthetics...323
- hardware separation.....282
- hardware tokens .....72, 271
- health impact .....62, 113
- hearing.....309, 312
- hemoglobin level .....85
- heterogeneity .....296
- high-risk individuals.....274

- 
- hive minds..... 34, 161
  - Holonomic Brain Theory..... 28, 148
  - honeyclients.....299
  - honeypots.....293
  - hormones ..... 61
  - host-based devices .....248
  - hosts .....110, 189
    - unwitting ..... 61
    - vs. users.....59
  - hosts .....59
  - human enhancement..... 28, 148, 156
  - humidity controls..... 233
  - hunger .....310, 313
  - hypnoprosthesis.....319
  - I/O device access.....302
  - ideational neuroprosthetics .....319
  - identification .....28, 268
  - identifier management .....270
  - imitative communications
    - deception .....301
  - Impersonation .....51
  - implant .....29
  - implantable computers.....32
  - implantable medical devices
    - (IMDs) ..... 19
  - inactivity logout ..... 273
  - incident handling .....262
  - incident monitoring.....263
  - incident reporting .....263
  - incident response .....261
    - testing .....262
  - indicators of compromise.....249
  - information at rest, protection of
    - ..... 295
  - information flow enforcement... 275
  - information leakage ..... 233
  - information security architecture
    - .....210
  - information spillage response ....264
  - information system security officer
    - (ISSO) ..... 198
  - infrared light..... 308, 311
  - inner ear .....313
  - input mechanisms.....114, 115
  - input modalities ..... 119
  - input validation.....252
  - insider threats ..... 265
  - inspection ..... 220
  - integrated situational awareness
    - ..... 246
  - integrity .....16, 39, 132, 142
    - checks ..... 250
    - software ..... 249
    - system and information..... 241
    - transmission ..... 289
  - intellectual property .....164
  - intelligence, all-source ..... 215
  - interbeat interval ..... 87
  - interconnections, system ..... 221
  - internal monologue ..... 320
  - interoception..... 310
  - interoceptive neuroprosthetics .. 310
  - interoesthetic neuroprosthetics . 313
  - intrusion alarms..... 230
  - intrusion detection ..... 245
    - automated..... 230
    - wireless..... 246
  - intrusion responses, automated 230
  - invasive device ..... 29
  - iris patterns ..... 84
  - jamming..... 51, 78
  - joint operation and use ..... 60
  - keystroke analysis..... 85
  - kinesics .....323
  - language..... 321
  - language of thought .....322
  - leakage, information.....233
  - learning capability, continuous..252
  - least functionality ..... 238
  - least privilege .....220, 277
  - licensing.....111
  - limitation of harm ..... 214
  - live data, use of ..... 218
  - local field potentials (LFPs) .....25
  - location of components ..... 233
  - lockable casings ..... 228
  - magnetic fields..... 308
  - magnetoesthetic neuroprosthetics
    - ..... 314

- magnetoreceptive neuroprosthetics .....308
- magnetoreceptors .....308
- maintenance .....111, 178, 240
  - personnel .....240
  - timely .....241
  - tools.....240
- malicious code analysis .....244
- malicious code protection .....242
- management controls .....205
- management cybernetics..... 101
- manipulative communications
  - deception .....301
- manufacturers .....109, 184
- mean time to failure (MTTF) .....65
- mean time to repair (MTTR).....66
- mechanoreceptive prosthetics ...309
- mechanoreceptors.....309, 310
- media protection .....259
- media sanitization.....260
- memories
  - implanted ..... 33, 154
- memory ..... 27, 149, 156, 317
- memory protection .....258
- metavolution.....98, 320
- metavolitional neuroprosthetics 320
- mind uploading ..... 99
- misdirection.....296
- mnemonic designer .....200
- mnemoprosthetics ..... 27, 317
- mobile code..... 291
- module coupling .....283
- monitoring .....179, 228
  - account .....274
  - incident.....263
  - information system.....244
  - physical access .....229
- morphology, device.....113
- motor neuroprosthetics..... 24, 320
- motor plant.....321
- muscles.....309
- nanorobots..... 33, 61, 90, 93, 98
- narcolepsy.....25
- neosomatic neuroprosthetics .....35
- network disconnect ..... 290
- neural computing .....119
- neurally augmented sexual
  - function (NASF).....25
- neurocybernetics .....101
- neuroeffector junction ..... 321
- neuromodulation ..... 200
- neuroprosthetic device, definition
  - of..... 21
- NIST Special Publication 800-53,
  - Rev. 4..... 17
- nociceptive neuroprosthetics .... 310
- nociceptors ..... 310
- nocioesthetic neuroprosthetics .. 313
- non-computing security methods 41
- noninvasive device..... 29
- non-organizational users .....277
- non-organizationally owned
  - systems..... 280
- non-persistence.....257
- non-privileged access .....277
- non-repudiation..... 281
- nonsignature-based detection... 243
- nose .....310, 311
- object reuse ..... 283
- oculesics.....323
- odor ..... 85
- off-line storage ..... 296
- olfactoesthetic neuroprosthetics 312
- olfactory bulb ..... 310, 312
- olfactory cortex ..... 312
- olfactory nerve ..... 310
- olfactory neuroprosthetics..... 310
- olfactory receptor neurons ..... 310
- ontologies, device .....102, 107
- operating system.....118
- operational controls .....223
- operations security (OPSEC) ..... 215, 299

- ophthalmoesthetic
  - neuroprosthetics .....311
- optic nerve .....23, 311
- oral verbal language .....321
- organismic continuity .....90
- orthoesthetic neuroprosthetics ..315
- orthopractic motor
  - neuroprosthetics ..... 324
- outgoing communications traffic,
  - restriction of threatening .....287
- out-of-band channels.....299
- output filtering ..... 257
- output mechanisms ..... 115, 229
- output modalities ..... 121
- owner
  - information ..... 197
  - information system..... 197
- ownership
  - of one's body ..... 164
  - of thoughts and memories.. 164
- P300 potential spikes .....88
- pacemakers ..... 19
- pain .....310, 313
- palprints .....84
- paralanguage..... 322
- parietal lobe .....312
- Parkerian Hexad .....130
- partially invasive device.....29
- partitioning, information system
  - .....297
- passive neuroprosthetics .....30
- password-based authentication .270
- passwords
  - memories as .....88
  - thoughts as .....88
- penetration testing..... 213, 222
  - facility ..... 229
- perceptual neuroprosthetics .....318
- permitted actions without
  - identification or authentication
    - .....278
- personal identity .....98
- personnel
  - sanctions ..... 227
  - screening..... 225
- security ..... 224
- photoreceptive neuroprosthetics
  - ..... 308
- photoreceptors..... 308
- physical access authorizations ...227
- physical connections, unauthorized
  - ..... 288
- physical neural networks ..... 92, 117
- physical protection .....227
- planning..... 208
- platform-independent applications
  - ..... 294
- portable storage devices..... 279
- ports .....114, 302
- position risk designation..... 224
- possession .....16, 134, 143
- post-employment requirements 226
- posthumanism .....15, 32, 95, 166
- power
  - emergency .....232
  - equipment and cabling ..... 231
  - supply ..... 114
  - transmission levels ..... 279
- predeployed keys ..... 71
- predictable failure prevention ... 254
- predictive maintenance..... 241
- presenter, neuroprosthetic device
  - as.....311
- pressure..... 309
- probationary periods ..... 248
- process isolation ..... 300
- processing site, alternate .....235
- proprioception ..... 309
- proprioceptive neuroprosthetics309
- proprioceptive system ..... 313
- proprioesthetic neuroprosthetics312
- prosthesis..... 29
- protected environments..... 251
- protocols, neuroprosthetic security
  - ..... 103
- providers, device .....184
- proximity verification .....75
- purge of mobile device .....277
- pyrometry ..... 309
- quantum computing..... 92

- queries .....78
- radio waves .....308
- randomizing of communications  
.....289
- receptors.....308
- recovery and reconstitution,  
    information system .....236
- red team exercises .....222
- rejectability .....16, 139, 142
- remapping of sense modalities ...315
- remediation, flaw .....241
- remote access.....243, 278
- residual information .....283
- restoration.....28
- retention, information .....254
- retinal implants .....19
- retinal patterns .....84
- reusability .....112
- RFID.....19, 43, 72
- risk assessment .....47, 173, 206
- risk management.....47, 96
- risks.....46
- rules of behavior .....209
- safe mode .....236
- sanitization, media.....181, 260
- sapient metavolitional agent, host  
    as .....17, 146, 147
- security assessments .....221
- security categorization .....172, 206
- security concept of operations  
    (CONOPS) .....209
- security engineering principles...212
- security function isolation.....282
- security function verification .....249
- security goals .....129
- prioritization of.....142
- security impact analysis.....237
- security policy filters.....276
- security testing and evaluation...213
- sense sculptors.....201
- sensors.....302
- sensory neuroprosthetics .....22, 307
- sensory playback.....33, 41, 80
- sensory substitution .....315
- separation of duties .....276
- separation of information flows 276
- session audit .....281
- session lock.....278
- session termination .....278
- shared resources .....283
- shielding  
    bandages .....75
- radio frequency.....75
- undershirt .....75
- shutdown on failure .....281
- signal parameter identification ..301
- simulated events .....261
- single-neuron action potentials ...25
- situational awareness .....246
- skeletal striated muscles .....309
- skin .....309
- smell.....310, 312
- social and economic actor, host as  
    .....17, 146, 159
- social exclusion .....166
- social relations .....160
- software .....249
- somatosensory system.....309
- sound waves .....309
- spam protection .....252
- spillage, information .....264
- spinal cord injury .....24
- spoofing .....78
- standby component installation 255
- steganography  
    cognitive .....248
- motor .....248
- storage site, alternate .....235
- stroke .....24
- subcutaneous buttons .....76
- substrate, computational .....116
- supply chain  
    coordination .....263
- protection.....214

- surveillance
  - equipment ..... 230
  - video ..... 230
- swallowing ..... 24
- swarms, nanorobotic ..... 92
- system development life cycle
  - (SDLC) ..... 171, 211
- system security plan ..... 208
- syzygocybernetics ..... 35
- tactioception ..... 309
- tactioceptive neuroprosthetics .. 309
- tactioesthetic neuroprosthetics .. 312
- tamper detection ..... 220
- tamper protection ..... 229
- tamper resistance ..... 220
- taste ..... 310, 312
- taste buds ..... 310
- tattoos
  - ultraviolet-ink ..... 74
  - visible ..... 74
- TCP/IP ..... 121
- technical controls ..... 267
- technical surveillance
  - countermeasures survey ..... 207
- telecommunications services ..... 235
- temperature ..... 86, 309, 313
  - controls ..... 233
- termination, personnel ..... 225
- thalamus ..... 313
- therapy ..... 28
- thermoceptive neuroprosthetics 309
- thermoesthetic neuroprosthetics 313
- thermograms ..... 84
- thermoreceptors ..... 310
- thin nodes ..... 293
- third-party credentials ..... 272
- thirst ..... 310, 313
- threat modeling ..... 218
- threat sources ..... 45
- threats ..... 46
  - insider ..... 49, 265
- time to remediate flaws ..... 242
- tone of voice ..... 322
- tongue ..... 310, 311
- tools, maintenance ..... 240
- touch ..... 309, 312
- traceability ..... 217
- traffic analysis ..... 247
- training
  - security awareness ..... 265
- training environments, automated
  - ..... 261
- training, incident response ..... 261
- transduction ..... 311
- transhumanism ..... 15, 95
- traumatic brain injury ..... 24
- trustworthiness ..... 217
- typologies ..... 102
- ultrasound ..... 311
- ultraviolet light ..... 308
- unauthorized commands, detection
  - of ..... 243
- unauthorized users ..... 44
- unsanctioned information,
  - detection of ..... 276
- unsuccessful logon attempts ..... 277
- unsupported system components
  - ..... 221
- updates
  - automatic software/firmware
    - ..... 242
- uploading, mind ..... 99
- usage restrictions ..... 238, 304
- USB flash drive ..... 46
- user-installed software ..... 239
- users ..... 59, 110, 188
  - vs. hosts ..... 59
- utility ..... 16, 136, 142
- vagus nerve stimulation (VNS) ..... 25
- validation, input ..... 252
- vascular patterns ..... 84
- ventilator ..... 24
- verification, security function .. 249
- vestibular nuclei ..... 309
- video games ..... 34
- violations, automated response. 250
- virtual reality ..... 34, 153, 156
- viruses
  - engineered ..... 90
- vision ..... 311



|                                                           |             |
|-----------------------------------------------------------|-------------|
| visitor access records .....                              | 230         |
| visual cortex .....                                       | 311, 314    |
| visuo-spatial sketchpad .....                             | 318         |
| vocal characteristics .....                               | 85          |
| voicebox .....                                            | 322         |
| vulnerabilities .....                                     | 45, 48, 167 |
| vulnerability analysis .....                              | 218         |
| vulnerability scanning .....                              | 207         |
| weakest link, human beings as the .....                   | 81          |
| wipe of mobile device .....                               | 277         |
| wireless access .....                                     | 279         |
| Wireless Identification and Sensing Platform (WISP) ..... | 79          |
| wireless link protection .....                            | 300         |
| Working Memory model .....                                | 318, 319    |
| written verbal language .....                             | 321         |
| xenergetic motor neuroprosthetics .....                   | 324         |
| xenesthetic neuroprosthetics .....                        | 315         |
| xenoception .....                                         | 311         |
| xenoceptive neuroprosthetics ....                         | 311, 315    |
| xenoceptor .....                                          | 311         |
| xenopractic motor neuroprosthetics .....                  | 324         |
| xenosensory neuroprosthetics ....                         | 316         |
| xenosomatics .....                                        | 34          |
| X-rays .....                                              | 308, 311    |

## About the Author

Matthew E. Gladden is cyberneticist whose research focuses on the managerial, organizational, and social implications and impacts of emerging technologies such as genetic engineering and biotechnology, nanotechnology, artificial intelligence, artificial life, social robotics, and augmented and virtual reality. He lectures internationally and his research has been published in journals such as the *Annals of Computer Science and Information Systems*, *International Journal of Contemporary Management*, and *Informatyka Ekonomiczna / Business Informatics*, as well as by IOS Press and The MIT Press. He is the founder and CEO of management consulting firms NeuraXenetica, LLC, and Cognitive Firewall, LLC, and has previously served as Associate Director for Programs, Administration, and Finance of the Woodstock Theological Center and Administrator of the Department of Psychology at Georgetown University. He has also taught philosophical ethics and worked in video game design. He is a member of ISACA, ISSA, and the Academy of Management.







How do we ensure information security for a computer that is entangled with the neural processes of a human mind – and for the human mind that is interconnected with such a device?

The need to provide information security for neuroprosthetic devices grows more pressing as increasing numbers of people utilize technologies such as cochlear implants, artificial retinas, robotic prosthetic limbs, and deep brain stimulation. Moreover, more advanced neuroprosthetic technologies designed for human enhancement are expected to someday transform their users' sensory, motor, and cognitive capacities in ways so radical that their nature can best be described as "posthuman." It is essential not only to ensure the information security of such neuroprosthetic devices themselves but – more importantly – to ensure the physical and psychological health, autonomy, and personal identity of the human beings whose cognitive processes are inextricably linked with such devices. Information security practitioners must not only guard against threats to the confidentiality and integrity of data stored within a neuroprosthetic device's internal memory; they must also guard against threats to the confidentiality and integrity of thoughts, memories, and desires existing within the mind of the device's human host.

This volume is the first book dedicated to studying these issues comprehensively from both theoretical and practical perspectives, and it establishes important new conceptual frameworks to guide the development of this emerging field. The book provides an introduction to the current state of neuroprosthetics and expected future trends, along with an introduction to fundamental principles of information security and an analysis of why they must be re-envisioned to address the unique challenges posed by advanced neuroprosthetics. A device ontology for neuroprosthetics is formulated, and a two-dimensional cognitional security framework is developed whose security goals are designed to protect a device's human host in his or her roles as a sapient metavolitional agent, embodied embedded organism, and social and economic actor. Detailed practical consideration is then given to information security responsibilities and to management, operational, and technical controls as they relate to neuroprosthetic technologies. Finally, a biocybernetic model is developed for classifying neuroprosthetic devices according to their participation in the neural activity of their human hosts.



ISBN 9780692501610



9 780692 501610

53495 >

